ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

ANÁLISIS DE CALIDAD DE SERVICIO EN TRANSFERENCIA DE VOZ Y VIDEO EN UNA RED DE TECNOLOGÍA MPLS (MULTI-PROTOCOL LABEL SWITCHING)

Trabajo de titulación presentado para optar al grado Académico de:

INGENIERO EN ELECTRÓNICA TELECOMUNICACIONES Y REDES

AUTOR: CROW SÁNCHEZ WALTHER ENRIQUE

TUTOR: ING. VINICIO RAMOS VALENCIA

Riobamba-Ecuador

2016

ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

FACULTAD DE INFORMATICA Y ELECTRÓNICA

ESCUELA DE INGENIERIA EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

El tribunal de trabajo de titulación certifica que: La Propuesta Tecnológica: ´´ANALISIS DE CALIDAD DE SERVICIO EN TRANSFERENCIA DE VOZ Y VIDEO EN UNA RED DE TECNOLOGIA MPLS (MULTI-PROTOCOL LABEL SWITCHING)", de responsabilidad del señor Crow Sánchez Walther Enrique, ha sido minuciosamente revisado por los miembros del tribunal de tesis, quedando autorizada su presentación.

NOMBRE	FIRMA	FECHA
Ing. Washington Luna **DECANO FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**	_____	_____
Ing. Franklin Moreno **DIRECTOR DE ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES**	_____	_____
Ing. Vinicio Ramos Valencia **DIRECTOR DEL TRABAJO DE TITULACIÓN**	_____	_____
Ing. Marcelo Donoso **MIEMBRO DEL TRIBUNAL**	_____	_____

Yo, Walther Enrique Crow Sánchez soy responsable de las ideas, doctrinas y resultados expuestos en esta propuesta tecnológica y el patrimonio intelectual de trabajo de titulación pertenece a la Escuela Superior Politécnica De Chimborazo.

_____

Walther Enrique Crow Sánchez

DEDICATORIA

A mis maestros que formaron parte de mi vida estudiantil, y que aportaron con sus conocimientos para cumplir una parte de mi vida, con mucho amor a Dios todopoderoso creador del universo, benévolo conmigo, por haberme colmado de bendiciones y fortalezas necesarias para emprender un buen camino en la vida, iluminando mis pasos día a día y hacer de mí un profesional. A mis padres, por ser parte fundamental en mi vida; un ejemplo a seguir; gracias a su amor, y su apoyo incondicional; he podido salir adelante, es a ellos a quien le dedico con todo el amor del mundo mi esfuerzo y mi carrera.

Walther

AGRADECIMIENTO

El más sincero agradecimiento a la Escuela Superior Politécnica De Chimborazo, por darme la oportunidad de obtener una profesión y ser una ayuda para la sociedad. A Dios, por haberme permitido la realización de esta investigación. A mis padres que gracias a su apoyo incondicional, a su perseverancia, a su entrega total de tiempo y voluntad, lograron que alcance uno de mis objetivos propuestos, constituyéndose en el más noble y verdadero ejemplo de amor puro y sincero. Agradezco, a mi asesor Ing. Vinicio Ramos Valencia por la motivación constante y haberme brindado las facilidades necesarias del caso. A la Escuela Superior Politécnica del Chimborazo, a La Escuela de Ingeniera en Electrónica, Telecomunicaciones y Redes a su cuerpo Docente por su valioso aporte de conocimientos. Es necesario reconocer el esfuerzo empleado en todo este proceso de enseñanza como aprendizaje, del cual orgullosamente formo parte y también a todas las personas que han colaborado en la elaboración de mi tesis.

Walther

TABLA DE CONTENIDO

Paginas

DERECHO DE AUTOR…….....ii

CERTIFICACIÓN……iii

DECLARACION DE RESPONSABILIDAD…….....iv

DEDICATORIA……v

AGRADECIMIENTO……...vi

TABLA DE CONTENIDO……..vii

INDICE DE FIGURAS……xii

INDICE DE TABLAS……xiii

INDICE DE ANEXOS……xv

RESUMEN..... xvi

SUMMARY xvii

INTRODUCCION xvii

CAPITULO I 8

1. MARCO TEORICO 8

1.1 Fundamentos MPLS 8

1.1.2 Función mpls..... 9

1.2 Arquitectura MPLS 10

1.2.1 OSPF 11

1.2.2 Algoritmo del estado de enlace 11

1.2.3 Algoritmo del trayecto más corto..... 12

1.2.4 Ventajas y Desventajas..... 13

1.3 BGP 13

1.3.1 SESIONES BGP 14

1.2.1 Routers MPLS 14

1.2.1.1 Label Switch Router 14

1.2.1.2 Label Edge Routers (LER) 15

1.2.1.3 Label Switched Path..... 15

1.2.3 Tipos de LSP MPLS ... 16

1.2.3.1 Ruteo hop-by-hop ... 16

1.2.3.2 Ruteo explícito ... 16

1.2.3.3 NHLFE (Next Hop Label Forwarding Entry) ... 16

1.2.3.4 Forwarding equivalence Class ... 16

1.2.4 Etiqueta ... 17

1.2.4.1 Estructura de etiquetas ... 18

1.2.5 Pila de etiquetas (LABEL STACK) ... 19

1.2.6 Nodos mpls ... 20

1.2.7 Distribución de etiquetas ... 20

1.2.7.1 Control de distribución de etiquetas ... 22

1.2.7.2 Protocolos para distribución de etiquetas. ... 23

1.2.7.3 Encapsulación de Etiquetas ... 23

1.2.7.4 Uniones a etiquetas ... 24

1.2.8 Clasificación de etiquetas ... 24

1.2.9 Mecanismos de señalización ... 24

1.3 Funcionamiento global ... 25

1.3.1 Construcción de tablas de encaminamiento. ... 26

1.3.2 Creación de rutas LSP's. ... 27

1.3.3 Construcción de LSP's ... 28

1.3.4 Inserción de etiquetas. ... 28

1.3.5 Envío de paquetes. ... 28

1.4 Aplicaciones de mpls ... 29

1.4.1 La ingeniería de tráfico ... 29

1.4.2 Aplicaciones de ingeniería de tráfico ... 31

1.4.3 Balanceo de carga ... 32

1.5 Calidad de servicio ... 32

1.5.1 Calidad de servicio (QoS) y clases de servicios (CoS) ***35***

1.5.2 Parámetros de calidad de servicio ***35***

1.5.3 Beneficios principales de QoS ***36***

1.5.4 Requerimientos de las clases de servicio CoS ***37***

1.5.5 Tecnologías para el soporte de QoS ***39***

1.5.5.1 Intserv y diffserv *40*

1.5.5.2 Arquitectura de servicios integrados *41*

1.5.5.3 Arquitectura diffserv *43*

1.6 Arquitectura mpls y calidad de servicio QoS en una red ip **44**

1.6.1 Codecs ***48***

1.6.1.1 G.711 *48*

1.6.1.2 G.729 *48*

1.6.1.3 GSM. *49*

1.6.1.4 ILBC. *49*

1.6.1.5 H.263 *49*

1.6.1.6 H.263p *50*

1.6.1.7 H.264 *50*

1.7 Elastix **51**

1.7.2 Ventajas ***51***

1.7.3 Desventajas ***51***

CAPITULO II **52**

MARCO METODOLOGICO **52**

2.1 Introducción **52**

2.2 Diseño de la arquitectura de red MPLS **52**

2.3 Desarrollo de la arquitectura de red emulada **53**

2.4 Direccionamiento **53**

2.5 Configuración de los equipos en GNS3 **54**

2.5.1 Verificación de la red OSPF *55*
2.5.2 Constatar red MPLS *55*
2.5.3 Verificar configuración de BGP *57*
2.5.3.1 Configuración del router PE-1 ..... *57*
2.5.3.2 Configuración del router PE-2 ..... *58*
2.5.3.3 Configuración de las vrf *58*
2.5.3.4 Verificar VRF *60*
2.6 Implementación en los equipos físicos **61**
2.6.1 Introducción *61*
2.6.2 Descripción de los routers *61*
2.6.3 Función de los routers *62*
2.7 Materiales para la conexión de los routers **63**
2.8 Conexión serial **63**
2.8.1 Conexión de las interfaces giga Ethernet *65*
2.9 Descripción de los switch **66**
2.10 Equipos adicionales **66**
2.10.1 Software y herramientas *67*
2.10.2 Virtualbox *67*
2.11 Elastix **67**
CAPITULO III **69**
3. MARCO DE RESULTADOS **69**
3.1 Introducción **69**
3.2 Conexión del servidor elastix **69**
3.2.1 Creación de los usuarios en elastix *70*
3.2.2 Activar servicio de video llamada *72*
3.3 Configuración de Softphone **74**
3.4 Pruebas de llamada VOIP **76**

3.5 Análisis 77

3.6 Captura de tráfico con WIRESHARK 78

3.7 Prueba de video llamada 80

3.8 Parámetros a evaluar 81

3.9 Resultados de los parámetros capturados de voz y video 81

3.9.1 Resultados de los parámetros al realizar una llamada de voip 81

3.9.2 Resultados de los parámetros al realizar una video- llamada 82

3.10 Evaluación de los parámetros obtenidos de voz y video 83

3.10.1 Evaluación de los parámetros obtenidos de voz 84

3.10.2 Evaluación de los parámetros obtenidos en video llamada 86

3.11 Consideraciones en base a los resultados 88

3.11.1 Características de los equipos 88

3.11.2 Consideraciones a nivel de software 88

3.11.3 Consideraciones de QoS a partir de los resultados obtenidos 89

CONCLUSIONES 90

RECOMENDACIONES 91

BIBLIOGRAFÍA

ANEXOS

INDICE DE FIGURAS

Figura 1- 1:Arquitectura de pruebas MPLS 6
Figura 2- 1:Funcionamiento MPLS 9
Figura 3- 1:Arquitectura MPLS 11
Figura 4- 1:Ejemplos de MPLS 17
Figura 5- 1:Situación de Etiquetas MPLS 18
Figura 6- 1:Etiqueta MPLS genérica 20
Figura 7- 1:Esquema de distribución 22
Figura 8- 1:Envió de paquetes MPLS 29
Figura 9- 1:Diagrama Ingeniera en Tráfico 31
Figura 10-1:Diagrama Modo de operación IntServ/DiffServ 44
Figura 1- 2:Diseño de la Arquitectura de la Red MPLS 53
Figura 2- 2:Direccionamiento 54
Figura 3- 2:Verificacion de OSPF 55
Figura 4- 2:Configuración de OSPF 56
Figura 5- 2:Figura de forwarding 56
Figura 6- 2:Conocimiento de LDP 57
Figura 7- 2:Configuración del router PE-1 58
Figura 8- 2:Configuración del Router PE-2 58
Figura 9- 2:Configuración VRF 59
Figura 10- 2:interfaces de VRF 59
Figura 11- 2:Redistribute connected 60
Figura 12- 2:Verificación VRF 60
Figura 13- 2:Voip y Trafico 61
Figura 14- 2:Router 2900 62
Figura 15- 2:Routers 63
Figura 16- 2:Conexión de cables seriales 64
Figura 17- 2:Interfaces Giga Ethernet 65
Figura 18- 2:Switch 66
Figura 19- 2:Virtualbox 67
Figura 20- 2:Elastix versión 2.5.0 68
Figura 21- 2:Interfaz web 192.168.0.150 68

Figura 1- 3:Usuario Elastix 70
Figura 2- 3:Campo de encriptación 71
Figura 3- 3:Reconocimiento del elastix 71
Figura 4- 3:Usuarios 72
Figura 5- 3:Usuarios utilizados en la llamada 72
Figura 6- 3:Activacion del servicio 73
Figura 7- 3:FREPBX 73
Figura 8- 3:Ventana del Codec de audio y video 74
Figura 9- 3:APP Zoiper 75
Figura 10- 3:Conexión de los usuarios al servidor 75
Figura 11- 3:Activación del codec de audio y video 76
Figura 12- 3:Enrutamiento de llamadas 77
Figura 13- 3:Software Ostinato 78
Figura 14- 3:Tráfico de paquetes 78
Figura 15- 3:Wireshark 79
Figura 16- 3:Protocolo SIP 79
Figura 17- 3:Llamada de video 80
Figura 18- 3 Protocolo RTP y códec de video 80
Figura 19- 3:Parámetros 82
Figura 20- 3:Paquetes Wireshark 83
Figura 21-3: porcentaje del análisis de voz 85
Figura 22-3: porcentaje de la evaluación de video 87

INDICE DE TABLAS

Tabla 1-1 Ventajas y Desventajas MPLS	13
Tabla 1-2 Direccionamiento	54
Tabla 2-2 Materiales	63
Tabla 3-2 Distribuciones de las conexiones	64
Tabla 4-2 Descripción de las interfaces	65
Tabla 5-2 Descripción de los Switch	66
Tabla 1-3 Escala cuantitativas y cualitativas	83
Tabla 2-3 Parámetros obtenidos y recomendados	84
Tabla 3-3 Ponderaciones	84
Tabla 4-3 Parámetros a evaluar video llamada	86
Tabla 5-3 Ponderaciones del análisis de video llamada	86

ÍNDICE DE ANEXOS

ANEXO A	Configuración de los routers
ANEXO B	Instalación de elastix

RESUMEN

Se diseñó e implemento una red Multiprotocol Label Switching (MPLS) para realizar el análisis de calidad de servicio al transferir audio y video, realizado con equipos CISCO en los laboratorios de la academia CISCO. En un principio se hizo un estudio sobre redes MPLS su configuración y funcionamiento al realizar el tráfico de los paquetes las ventajas que brinda a diferencia de una red ip, posterior se procedió a diseñar la red, probar los comandos de configuración haciendo uso de un emulador de redes como es GNS3 de esta manera se harían las pruebas de conectividad y convergencia de cada protocolo y sistema configurado para evitar errores de comunicación al configurar con los equipos físicos de CISCO, la red hizo uso del protocolo ospf para establecer la comunicación entre los router necesario para que converja MPLS. MPLS se configuro en cada interfaz de la red para asegurar el empaquetamiento LDP en todos los extremos, se hizo uso del protocolo BGP para poder crear los routers PE de extremo a extremo (servidor- cliente). BGP permitió utilizar el MP-BGP familia del mismo protocolo así establecer las vrf para aislar el tráfico y balancear la carga. Luego se configuro y creo usuarios para realizar llamadas de audio y video con el servidor ELASTIX conectando a la red a través de su vrf tanto para el servidor como los clientes. Se inyecto un tráfico externo para el análisis de un tráfico real y no ideal. Se analizó los datos obteniendo como resultado jitter: 27.70ms, latencia Max: 608.73ms, perdida de paquetes: 0% comparándolos con valores mínimos que determinen una calidad aceptable. Con los equipos cisco se pudo implementar la red MPLS para el análisis de calidad de servicio. Antes de implementar la red es recomendable realizar pruebas en un emulador para evitar daños en equipos.

PALABRAS CLAVES: <TECNOLOGIA Y CIENCIAS DE LA INGENIERIA>, <TECNOLOGIA DE COMUNICACIONES>, <MULTIPROTOCOL LABEL SWITCHING [MPLS]>, <ANALISIS DE CALIDAD >, <TRANSFERIR AUDIO Y VIDEO, <INYECTOR DE TRAFICO>, <VIRTUAL ROUTING AND FORWARDING [VRF]>.

SUMMARY

An MPLS Multiprotocol Label Switching Network was designed and implemented to analyze the service quality when transferring audio and video, this was carried out with the use of CISCO equipment at the laboratories of CISCO academy. At the beginning an MPLS study was carried about its setting and working when sending packets of data as well as the advantages offered in relation to an ip network, then the network was designed and the setting commands were tested using a GNS3 network emulator, in this way the connectivity and convergence tests would be done for each protocol and system configured to avoid communication mistakes when they are configured with CISCO physical equipment. The network used the ospf protocol to establish the communication among the routers, this was necessary for MPLS to converge. MPLS was configured in each interface of the network to assure the LDP packaging on its borders and BGP protocol was used to create the PE routers from one border (server) to the other (customer). BGP allowed using MP-BGP the same protocol family to establish the vrf in order to separate the traffic and balance the packets of data. Then the users were created and configured to make audio and video calls with ELASTIX server connected to the network through its vrf for both server and customer. An external traffic was injected to carry out a real traffic, not an ideal one. The data were analyzed and the jitter result was: 27.70 ms, latency max 608.73 ms, packets lose 0%, this compared with the minimal values which determine an acceptable quality. With CISCO equipment, it was possible to implement the MPLS network to analyze the service quality. Before implementing the network, it is necessary to carry out tests with the use of the emulator in order to avoid damage in the equipment.

KEY WORDS: <TECHNOLOGY AND ENGINEERING SCIENCE>, <COMMUNICATIONS TECHNOLOGY>, <MPLS MULTIPROTOCOL LABEL SWITCHING>, <QUALITY ANALYSIS>, <TRANSFER AUDIO AND VIDEO>, <TRAFFIC INJECTOR>, <VIRTUAL ROUTING AND FORWARDING (VRF) >.

INTRODUCCION

Internet se ha transformado en los últimos años en una red de muy alta difusión en cuanto al número de usuarios conectados. Esto ha sido visto por parte de los operadores como una oportunidad de ofrecer nuevos servicios a dichos usuarios además del tradicional servicio de email, ftp y navegación Web. Algunos de estos servicios son por ejemplo servicios de telefonía, videoconferencia, televisión, radio, etc.

Estos nuevos servicios presentan requerimientos diferentes en cuanto a volumen de tráfico, calidad de servicio y seguridad. Internet no fue pensada por sus diseñadores originales para trabajar en este contexto de servicios sino en un contexto académico con intercambio de información del tipo emails, o ftp. El paradigma en que se ha basado el envío de paquetes en una red IP (protocolo base de Internet) ha sido la denominada política 'Best effort'. (Lloyd, 2001, p.87)

Best effort implica que el usuario envía paquetes y la red y esta hace su mejor esfuerzo para hacerlos llegar al destinatario, no asegurando ningún tipo de calidad del servicio (perdidas, retardos, etc.). Con este principio no es posible ofrecer servicios con requerimientos fuertes de Calidad de Servicio (QoS) en cuanto a perdidas retardos o jitter como exigen por ejemplo los servicios de voz o video interactivo. Protocolos superiores a IP (como TCP) han procurado solucionar el problema de la perdida de paquetes básicamente reenviando paquetes si estos no llegan a destino. (Abdelali, 2013, p.18)

Esto resuelve los problemas de la transferencia tradicional de datos, pero este tipo de protocolos no puede ser usado para la transferencia de servicios interactivos en línea, en los que no es posible esperar por una retransmisión. La comunidad de Internet ha realizado esfuerzos diversos en los últimos años para romper el paradigma actual y aproximarse a la calidad de servicio brindada por Red Publica Telefónica (PSTN). (Abdelali, 2013, p.18)

El problema que hoy se plantea es diseñar la nueva arquitectura, las políticas, las metodologías y las herramientas necesarias para desplegar una red multiservicio capaz de asegurar los requerimientos de QoS necesarios para cada uno de los servicios ofrecidos. Muchos de los esfuerzos realizados para transformar IP en una red de servicio convergente están aún en su fase experimental y no han logrado imponerse de forma masiva.

En paralelo nuevas propuestas surgen frecuentemente, fruto de una fuerte investigación en esta área. Aspectos básicos sobre cómo asegurar calidad de servicio en Internet, como medirla o estimarla, que protocolos o tecnologías usar para brindar estos servicios aun generan controversias. Eso abre las puertas a un campo donde hoy se encuentra un fuerte desarrollo académico y comercial. Como mencionábamos, se han propuesto diferentes modelos para brindar QoS en redes IP.

El primer modelo propuesto fue el de Servicios Integrados (IntServ), el cual procuraba establecer para cada flujo reserva de los recursos necesarios a lo largo de la red, para asegurar la calidad de servicio requerida. Este modelo tiene problemas de escalabilidad reserva de recursos por flujo y por lo tanto se lo ha dejado de ver como una solución posible en el corazón de Internet donde convergen millones de flujos. (Abdelali, 2013, p.18)

Recientemente ha cobrado fuerte desarrollo el modelo de Servicios Diferenciados (DiffServ). Este modelo busca solucionar los problemas de escalabilidad de IntServ agregando los flujos en clases y procurando dar calidad de servicio a cada clase según los requerimientos de la misma. DiffServ es un área de importante desarrollo actual en relación a Internet. Sin embargo, DiffServ no es suficiente en IP para poder asegurar QoS. (Hesselbach, 2001, pp.13-15)

Esto se debe a que con los protocolos actuales de ruteo IP se termina tráfico en ciertas zonas de la red aunque otras estén subutilizadas. Por este motivo la calidad de servicio aun para las clases de más alta prioridad de DiffServ se puede deteriorar. Como consecuencia, para poder asegurar QoS en IP es necesario realizar ingeniería de tráfico. Ingeniería de tráfico significa ser capaz de distribuir el tráfico que arriba a la red de manera eficiente dentro de la misma. (Hesselbach, 2001, p.15)

Tradicionalmente la ingeniería de tráfico en IP se realizó usando el modelo IP sobre ATM. Esta arquitectura tiene diversos problemas. Los principales problemas están referidos a la gestión de dos redes (IP y ATM), a la escalabilidad de la red y a la performance en redes de alta velocidad por la adaptación de la capa IP a la capa ATM. La Arquitectura MPLS (MultiProtocol Label Swiching) es una nueva arquitectura que habilita a realizar Ingeniería de Trafico en redes IP. (Hesselbach, 2001, p.13)

La característica principal de MPLS que habilita a realizar ingeniería de tráfico es la de ruteo explícito. El ruteo explicito permite establecer caminos (Label Switch Path, LSP) predefinidos para los paquetes. Esto se realiza desde los routers de la frontera de la red. MPLS retoma en este sentido las bases sobre las que se diseñó ATM, al establecer caminos virtuales para los flujos agregados.

Sin embargo MPLS se integra dentro de la tecnología IP, no requiriendo el despliegue, la operación y la gestión de una tecnología diferente como era el caso de IP over ATM. Al realizar ingeniería de tráfico en MPLS se genera la posibilidad de usar esta arquitectura para asegurar Calidad de Servicio. Esto se debe a que en el ruteo IP actual, los paquetes se envían por la ruta de menor número de saltos generando tráfico en ciertas zonas de la red y zonas donde la red esta subutilizada.

Las funciones de ruteo explícito de MPLS permiten enviar los paquetes por una ruta preestablecida o que se obtenga la misma analizando la carga de la red.

Formulación general del proyecto del trabajo de titulación

Planteamiento del problema/Antecedentes

La evolución constante de las tecnologías de conectividad intenta dar soluciones a los problemas que presentan la sociedad, la industria y las compañías. En un pasado la prioridad era la necesidad de procesar y almacenar información, con lo que nacieron los equipos informáticos individuales, posteriormente surgió la necesidad no sólo de procesar y almacenar la información sino que además era preciso ofrecer calidad de servicio en tiempo real por ello surgieron protocolos que garanticen la convergencia optima en una red. (Avallone, 2009, p.9)

En un principio las Redes IP solo ofrecían una clase de servicio Best Effort, pero actualmente se desea manejar todo tipo de tráfico como lo es voz, datos y video, por lo que se ha pensado que MPLS es la solución a todos estos inconvenientes, ya que con el Modelo DiffServ (Servicios Diferenciados) se puede clasificar el tráfico con diferentes prioridades según las necesidades del usuario. (Loshin, 2008, p. 77)

Los requerimientos de calidad de servicio (en adelante QoS) han cambiado con el transcurso de los años, inicialmente las exigencias de información se encontraban básicamente en el transporte de información masiva que para la época resultaba novedosa y muy efectiva, además la cantidad de usuarios era muy pequeña; sin embargo, las necesidades han ido evolucionando y actualmente la demanda de acceso a los datos en el momento oportuno es una necesidad que debe ser garantizada al usuario final. Por tal razón se considera imprescindible la reserva de recursos para los contenidos sensibles circundantes dada la cantidad de tráfico existente en la Internet. (Loshin, 2008, p. 77)

Dentro de los estándares que podrían soportar estas exigencias establecidas por los usuarios esta la Conmutación de Etiquetas Multiprotocolo (MPLS), la Conmutación de Etiquetas Multiprotocolo Generalizado (GMPLS) y la Conmutación de Etiquetas Multiprotocolo con Perfil de Transporte (MPLS-TP). (Avallone, 2009, p.9)

Específicamente una de las grandes virtudes de MPLS es que cada Camino virtual de Conmutación de Etiquetas (LSP) puede estar asociado a varias Clases Equivalentes de Envío (FEC), pudiéndose asignar tantos flujos de información a cada FEC como sea necesario. Esto conlleva a que, a efectos prácticos, pueda elegirse qué tráfico va a ser encaminado por qué LSP en concreto, pudiendo implicar éste solo hecho la alteración de la QoS ofertada. (Avallone, 2009, p.9)

Si además a la estructura MPLS se le asocia con Diffserv se resuelve gran parte de los problemas de QoS en las redes, ya que los servicios diferenciados utilizan el campo Tipo de Servicio para clasificar los flujos en diferentes clases en los nodos de ingreso al dominio. (Avallone, 2009, p.9)

De acuerdo a lo anteriormente mencionado se propone un caso de estudio que permita analizar las características que ofrece la conmutación de etiquetas al transmitir voz y video cuando se intenta implementar la priorización y diferenciación de los flujos a fin de dotar a MPLS de QoS. (Thomas, 2006, p.35)

Formulación del problema

¿Es posible medir la calidad de servicio en la transferencia de voz y video para una red basada en la tecnología MPLS?

Sistematización del problema

¿Se podrá identificar los factores que afecten la calidad de servicio en redes basadas en el protocolo MPLS?
¿Cómo se determinaran los parámetros y la forma de medición de la calidad de servicio en redes basadas en el protocolo MPLS?
¿Qué software o hardware se necesitara para implementar una red MPLS?
¿Cómo influirá el tráfico de voz y video en el ancho de banda de la red MPLS?
¿Qué configuraciones se deberá realizar para implantar el protocolo MPLS en una estructura de red?

¿Cómo se evaluara la calidad de servicio en la red de Core mpls?

Justificación del trabajo de titulación

Justificación teórica

La presente investigación se enfoca a la calidad de servicio que puede ofrecer el protocolo MPLS al realizar la transferencia de voz y video, además del control de la tasa de paquetes entregados, latencia y jitter, ya que en su pasado las compañías luchaban por ofrecer velocidad y ancho de banda en sus conexiones pero con el desarrollo de la fibra óptica estos parámetros ya no parecían ser un problema. Entonces, el nuevo parámetro de competencia es la calidad de servicio por eso es el caso de estudio del presente proyecto y se utilizó el protocolo MPLS por sus garantías que ofrece en el óptimo tráfico de paquetes. (Gallear, 2002, p. 10)

Debido a este gran interés que se maneja al momento de ofrecer un servicio de conectividad, existe la necesidad de investigar los aspectos básicos de cómo asegurar la QoS, los parámetros que afectan al rendimiento, como estimarlos, y cuáles son las ventajas que nos brinda la aplicación de un protocolo como es MPLS para contrarrestar sus efectos negativos. (Lloyd, 2001, p.81)

Teniendo claro que se requiere tecnología de arquitectura de red con mayores prestaciones, la principal herramienta para el proyecto será el protocolo MPLS (MultiProtocol label switching). El cual posee la característica de poder realizar una eficiente ingeniería de tráfico por medio de herramientas como el ruteo explicito, y así abrir la posibilidad de ofrecer la calidad de servicio esperada al momento de realizar el tráfico de voz y video como una de las nuevas necesidades del mercado. (Gallear, 2002, p. 10)

Justificación aplicativa

La implementación de las herramientas para estudiar la calidad de servicio requiere en primera instancia del análisis del protocolo MPLS, como es su encaminamiento y etiquetado, y si soportara el tráfico de voz y video, para instalar el software necesario que hará la capturar de todos los posibles paquetes generados. Posteriormente diseñar la estructura de la red que soportara el protocolo MPLS y el periodo de estudio que se llevaría a cabo para recolectar los suficientes datos y poder determinar la QoS que tendremos al realizar un tráfico de voz y video.

Es importante recalcar que la integración de MPLS y DIFFSERV mejora las prestaciones de calidad que el tradicional servicio que se ha ofrecido a la mayoría de ISPs actualmente, se combina el tratamiento diferenciado de los agregados de tráfico entregado por la arquitectura de DIFFSERV y la simplificación de los procesos de enrutamiento proporcionado por la tecnología MPLS.

Existe una variedad de herramientas para el análisis de QoS, sin embargo no todos ofrecen la posibilidad de manipular todas las variables de acuerdo a las necesidades, la tentativa de herramienta a utilizar para recopilar datos son: Netperf, D-ITG, NetStress, MGEN, LANforge, Network Traffic Generator, Rude & Crude, WlanTV, OPNET Modeler, Cisco SAA, VVQManager, TamoSoft Throughput Test, Iperf, GNS3, de software a utilizar.

Permiten realizar análisis de algunos parámetros de QoS y de entre una herramienta a otra los resultados pueden diferir ya que cada uno maneja diferentes algoritmos y procesos para obtener resultados, la interfaz gráfica también es importante debido que algunos ofrecen solamente la consola, otros interfaz gráfica y algunos ambos, en otros casos el proceso de implementación son muy complejos; en el caso de emuladores de dispositivos de red.

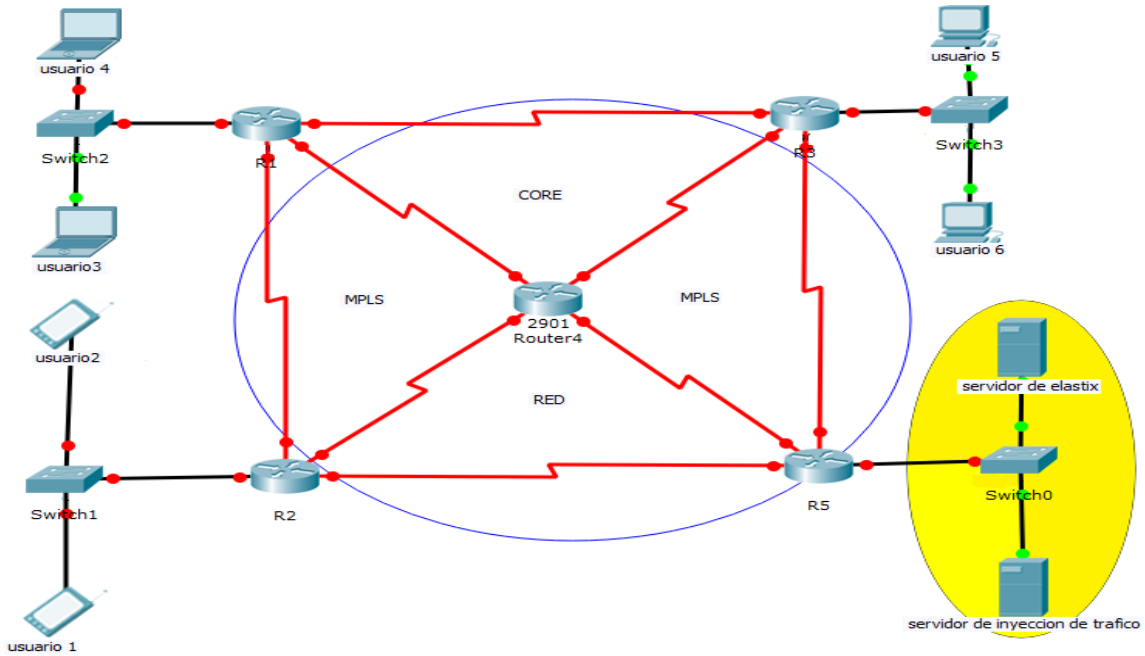


Figura 1- 1: Arquitectura de pruebas MPLS

Fuente: Crow. W 2016

Objetivos

Objetivos generales

- Analizar la calidad de servicio en la transferencia de voz y video en una red de tecnología MPLS (Multi-Protocol label switching).

Objetivos específicos

- Estudiar los conceptos fundamentales sobre calidad de servicio, herramientas de captura/inyección y el proceso de enrutamiento de datos en redes MPLS.

- Implementar una red MPLS que a través de herramientas de inyección de tráfico visualicen el comportamiento de paquetes de audio y video.

- Evaluar los resultados obtenidos en las pruebas realizadas en los escenarios sobre los parámetros de latencia, jitter, tasa de paquetes de los datos capturados en redes MPLS.

- Proponer las consideraciones mínimas para asegurar la QoS en audio y video sobre redes MPLS.

CAPITULO I

1. MARCO TEORICO

1.1 Fundamentos MPLS

MPLS quiere decir Conmutación de Etiquetas Multiprotocolo (Multiprotocol Label Switching), es una tecnología relativamente nueva que se desarrolló para solucionar la mayoría de los problemas que existen en la técnica actual de reenvío de paquetes. La IETF cuenta con un grupo de trabajo MPLS que ha unido esfuerzos para estandarizar esta tecnología.

La mayoría de los protocolos de enrutamiento desarrollados en la actualidad están basados en algoritmos diseñados para obtener el camino más corto para el recorrido del paquete por la red y no toman en cuenta parámetros adicionales como son retardo, jitter, y congestión de tráfico, los cuales pueden afectar el desempeño de la red, por lo que la ingeniería de tráfico es un reto para los administradores de redes.

MPLS actúa como nexo entre los protocolos de red y el correspondiente protocolo de nivel de enlace. Para ello, en la estructura de una trama, se sitúa la cabecera MPLS después de la cabecera de nivel de red y antes de la cabecera de nivel de enlace. De hecho, el reenvío de paquetes MPLS está basado en etiquetas y no en el análisis de los datos encapsulados desde niveles superiores.
Es una tecnología multiprotocolo que admite cualquier protocolo de red, pero al mismo tiempo permite cualquier tecnología en capas inferiores.

De esta forma, se ha proporcionado un atractivo mecanismo para aprovechar la infraestructura actualmente desplegada en ámbitos troncales, facilitando así la migración de tecnologías; sin embargo, los esfuerzos realizados desde hace años para desarrollar mecanismos innovadores que den soporte a IP sobre ATM no se han perdido, ya que la mayoría de las técnicas desarrolladas son válidas para disponer de IP sobre MPLS y MPLS sobre ATM. (Damon, 2002, pp. 8-9)

La adición del envío de paquetes basado en etiquetas complementa el enrutamiento convencional pero no lo reemplaza. MPLS es un trabajo realizado y especificado por la Internet Engineering

Task Force (IETF) que da los parámetros para la eficiente designación de ruteo, envío y conmutación de tráfico que fluye por la red. (Gallear, 2002, p. 10)

1.1.2 Función mpls

• Permite especificar mecanismos para la administración de flujos de tráfico de diferentes tipos.
• Permanece independiente de los protocolos de capa 2 y de capa 3.
• Dispone de medios para traducir las direcciones IP en etiquetas simples de longitud fija utilizadas en diferentes tecnologías de envío y conmutación de paquetes.
• Tiene interfaces con protocolos de ruteo existentes como el Resource Reservation Protocol (RSVP), Border Gateway Protocol (BGP) y el Open Shortest Path First (OSPF).
• Soporta los protocolos de la capa de enlace usados tradicionalmente para IP. Además opera perfectamente sobre ATM y Frame Relay, dado el parecido en el mecanismo de transporte y conmutación.
• Diferentes tipos de tráfico requieren diferentes características de servicio, las cuales deben de ser garantizadas a lo largo de todo el camino a través de la red. MPLS permite la creación de caminos LSP (Label Switched Path) con características de servicios diferentes. (Hesselbach, 2001, pp.13-15)

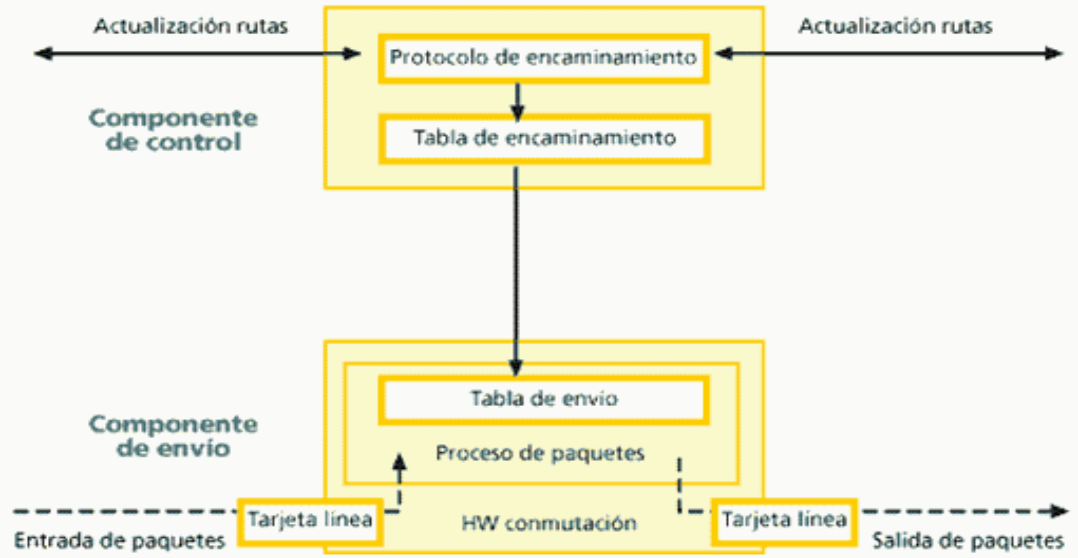


Figura 2- 1 Funcionamiento MPLS
Fuente:(Open SimMPLS, 2000)

1.2 Arquitectura MPLS

MPLS un concepto muy importante es el de LSP (Label Switch Path), que es un camino de tráfico específico a través de la red MPLS, el cual se crea utilizando los LDPs (Label Distribution Protocol), tales como RSVP-TE (Reservation Protocol – Traffic Engineering) o CR-LDP (Constraint-Based Routing – Label Distribution Protocol); siendo el primero el más común. El LDP posibilita a los nodos MPLS descubrirse y establecer comunicación entre sí con el propósito de informarse del valor y significado de las etiquetas que serán utilizadas en sus enlaces contiguos.

Es decir, mediante el LDP se establecerá un camino a través de la red MPLS y se reservarán los recursos físicos necesarios para satisfacer los requerimientos del servicio previamente definidos para el camino de datos.

Una red MPLS está compuesta por dos tipos principales de nodos, los LER (Label Edge Routers) y los LSR (Label Switching Routers).Los dos son físicamente el mismo dispositivo, un router o switch de red troncal que incorpora el software MPLS; siendo su administrador, el que lo configura para uno u otro modo de trabajo.

Los nodos MPLS al igual que los "routers" IP normales, intercambian información sobre la topología de la red mediante los protocolos de encaminamiento estándar, tales como OSPF (Open Shortest Path First), RIP (Routing Information Protocol) y BGP (Border Gateway Protocol), a partir de los cuales construyen tablas de encaminamiento basándose principalmente en la alcanzabilidad a las redes IP destinatarias.

Teniendo en cuenta dichas tablas de encaminamiento, que indican la dirección IP del siguiente nodo al que le será enviado el paquete para que pueda alcanzar su destino final, se establecerán las etiquetas MPLS y, por lo tanto, los LSP que seguirán los paquetes. No obstante, también pueden establecerse LSP que no se correspondan con el camino mínimo calculado por el protocolo de encaminamiento. (Hesselbach, 2001, pp.13-15)

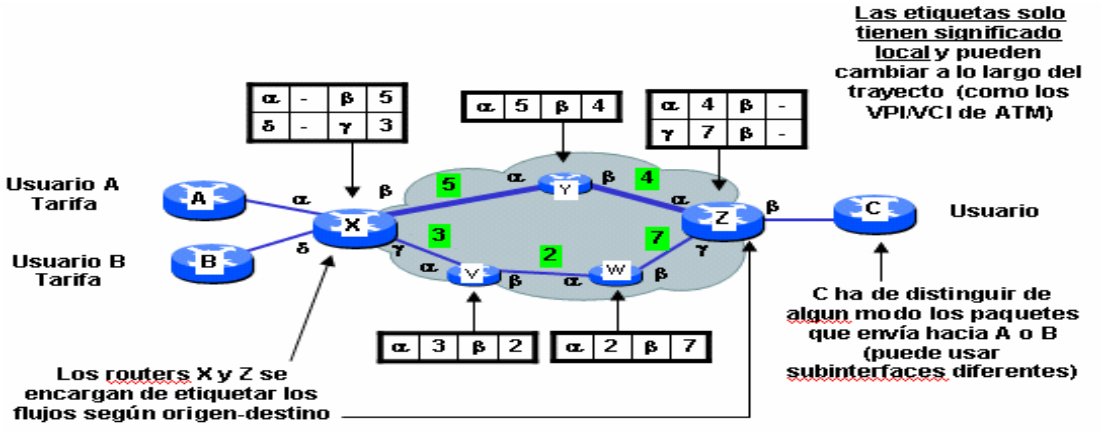


Figura 3- 1: Arquitectura MPLS

Fuente:(Ingeniería La Salle, 2000)

1.2.1 OSPF

Open Shortest Path First (OSPF), es un Protocolo de Gateway interior que se usa para distribuir información de enrutamiento dentro de un sistema autónomo único. El protocolo OSPF se basa en tecnología de estado de enlace, la cual es una desviación del algoritmo basado en el vector Bellman-Ford que se usa en los protocolos tradicionales de enrutamiento de Internet.

OSPF utiliza el algoritmo SPF y presenta tres versiones: OSPFv1, OSPFv2 y OSPFv3. Entre las características que presenta este protocolo de encaminamiento interior, se pueden citar las siguientes:

- Convergencia más rápida y sin crear ciclos.
- Soporte de métricas múltiples.
- Soporte de varias rutas a un mismo destino.
- Representación independiente para las rutas externas.
- Es jerárquico, es decir, permite la posibilidad de dividir un Sistema Autónomo en varias áreas.
- Utiliza IP directamente, es decir, no usa ni TCP ni UDP.
- Los subprotocolos que presenta son Hello Protocol, Exchange Protocol y Flooding Protocol (Duarte, 2014, p.78)

1.2.2 Algoritmo del estado de enlace

OSPF usa un algoritmo de estado de enlace para generar y calcular el trayecto más corto a todos los destinos conocidos. El algoritmo en sí mismo es bastante complicado. A continuación se ofrece una forma simplificada de nivel muy elevado para analizar los diversos pasos del algoritmo:

- Durante la inicialización, o bien cuando se produce algún cambio en la información de enrutamiento, un router generará un anuncio de estado de enlace. Este anuncio representará la agrupación de todos estos estados de enlace en dicho router.

- Todos los routers intercambiarán estados de enlace mediante la inundación. Cada router que recibe una actualización de estado de enlace debe almacenar una copia de su base de datos de estados de enlace y luego propagar la actualización a otros routers.

- Una vez que la base de datos de cada router está completa, el router calculará un árbol de trayecto más corto a todos los destinos. Para ello, el router utiliza el algoritmo Dijkstra. Los destinos, el costo asociado y el siguiente salto (next hop) para alcanzar dichos destinos formarán la tabla de IP Routing.

- En caso de que no se produzcan cambios en la red OSPF, por ejemplo, el costo de un enlace o bien la adición o eliminación de una red, OSPF debería permanecer muy tranquilo. Los cambios que se produzcan se comunicarán a través de paquetes de estado de enlace y se volverá a calcular el algoritmo Dijkstra para encontrar el trayecto más corto. (Duarte, 2014, p.78)

1.2.3 Algoritmo del trayecto más corto

El trayecto más corto se calcula con el algoritmo Dijkstra. El algoritmo coloca cada router en la raíz de un árbol y calcula el trayecto más corto a cada destino en función del costo acumulado requerido para alcanzar dicho destino. Cada router dispondrá de su propia vista de la topología, a pesar de que todos los routers crearán un árbol de trayecto más corto con la misma base de datos de estados de enlace. Las secciones siguientes indican que comprende la creación de un árbol de trayecto más corto. (Kumaki, 2004, p. 89)

1.2.4 Ventajas y Desventajas

Tabla 1-1 Ventajas y Desventajas MPLS

Ventajas	Desventajas
Utilización de métricas de costo para elección de las	**Requieren mayor capacidad**
Utilización de actualizaciones generadas por eventos e	**Requieren un diseño jerárquico estricto de red**
Cada router posee una imagen completa y sincronizada de la red	**Para administrar la red se requiere un conocimiento suficiente de los protocolos**
Admiten CIDR[1] y VLSM	**La inundación inicial de LSA reduce significativamente la capacidad de la red para**

Realizado por:(Walther Crow)

1.3 BGP

Border Gateway Protocol) El protocolo BGP garantiza el intercambio de información de enrutamiento libre de lazos (conocidos como loops) entre sistemas autónomos (AS), su función no es encontrar una red específica sino proporcionar información que permita encontrar el AS en el cual se encuentra dicha red, para lo cual el encargado de encontrar la red es el protocolo de pasarela interna a utilizar, tal como RIP, IGP, EIGRP, IS-IS, OSPF etc. BGP es un protocolo extremadamente complejo usado en Internet y dentro de las empresas multinacionales, permite políticas de enrutamiento y diferenciación entre el tráfico de diferentes proveedores de servicio.

Se dice que BGP es un protocolo de encaminamiento vectorial, porque almacena la información de encaminamiento como combinación entre el destino y las características de la ruta para alcanzar ese destino. El protocolo utiliza un proceso de selección determinista de la ruta para seleccionar la mejor dentro de las rutas factibles múltiples, usando las cualidades de la ruta como criterios. Las características como por ejemplo el retardo, la utilización del enlace o el número de saltos no se consideran dentro de este proceso. (Loshin, 2008, p. 77)

1.3.1 SESIONES BGP

En una sesión BGP participan sólo dos routers (peers). En cualquier momento una red puede tener muchas sesiones BGP concurrentes y también una misma pasarela puede participar en muchas sesiones BGP. En la sesión BGP se lleva a cabo el proceso denominado peering, que consiste en que un AS informa a otro sobre las redes que puede alcanzar a partir de éste.

Además de las sesiones inter-AS, los routers de borde de un mismo AS deben intercambiar también informaciones BGP para conocer las mismas rutas externas e internas. Para ello se utiliza el protocolo I-BGP, definido en la versión 4 de BGP, que utiliza el mismo tipo de mensajes que E-BGP, el cual es el protocolo utilizado en las sesiones BGP entre dos pasarelas de dos AS distintos. Según la especificación de BGP- 4, existe una diferencia a la hora de re anunciar rutas en E-BGP y en I-BGP.

En E-BGP, los prefijos que aprende un router de un vecino pueden ser anunciados a otro vecino mediante I-BGP y viceversa, pero un prefijo aprendido de un vecino mediante I-BGP no puede re anunciar a otro vecino por I-BGP. Esta regla de limitación para re anunciar prefijos entre routers vecinos mediante I-BGP sirve para evitar bucles (loops) dentro de un AS. (Satish, 2001, p. 12)

1.2.1 Routers MPLS

Los dispositivos que participan en los mecanismos del protocolo MPLS, pueden ser clasificados en ruteadores de etiqueta de borde o label edge routers (LERs), y en ruteadores de conmutación de etiquetas o label switching routers (LSRs). (Rossen, 2001, pp.13-15)

1.2.1.1 Label Switch Router

Son los que representan el núcleo de la red (backbone), los LSR son Router de gran velocidad en el núcleo de la red MPLS. Sus principales funciones son: participar en el establecimiento de los circuitos extremo-extremo de la red o LSPs (Label Switch Path) usando un protocolo de señalización apropiado y conmutar rápidamente el tráfico de datos entre los caminos establecidos.
En una red MPLS existen dos tipos de LSR:

- Label Edge Routers (LER): situados en los extremos de la red MPLS, son el nexo con las redes tradicionales (Ethernet, Frame Relay, ATM).

- Intermediate LSR: situados dentro de la red MPLS, reciben y transmiten los paquetes etiquetados por los enlaces correspondientes. Un LSR es capaz de realizar tres operaciones básicas: añadir (push), eliminar (pop) e intercambiar (swap) etiquetas MPLS.

La acción de añadir la primera etiqueta a un paquete se denomina imposición. Y la acción de eliminar la última etiqueta de un paquete se denomina disposición. (Rossen, 2001, pp.13-15)

1.2.1.2 Label Edge Routers (LER)

LER (Label Edge Router): Es un dispositivo que opera en el borde de la red de acceso y el dominio MPLS, el cual se encarga de insertar las etiquetas basándose en la información de enrutamiento. Un LER soporta múltiples puertos conectados a redes distintas (como pueden ser ATM, Frame Relay y Ethernet) y envía este tráfico a través de la red MPLS después de haber establecido un LSP (camino) utilizando un protocolo de distribución de etiquetas, también se encarga de retirar las etiquetas y distribuir el tráfico a las redes de salida. (Peter, 2003: 33)

1.2.1.3 Label Switched Path

LSP (Label Switched Path): Se llama así a cada uno de los caminos unidireccionales que un paquete toma para ir desde un LER de entrada a un LER de salida, pasando por uno o varios LSRs, es decir es un circuito virtual que siguen por la red todos los paquetes asignados a la misma FEC ("Forwarding Equivalente Class", Clase de Envío Equivalente). Al primer LSR que interviene en un LSP se le denomina de entrada o de cabecera y al último se le denomina de salida o de cola. Los LER de entrada y cola se encuentran en el exterior del dominio MPLS, el resto de dispositivos entre ambos son LSRs interiores del dominio MPLS.

En el interior de la red, los conmutadores de etiquetas ignoran la cabecera de la capa red de los paquetes y simplemente envían el paquete usando el algoritmo de etiquetas. Así los proveedores de servicio pueden diseñar LSPs personalizados que soporten aplicaciones y requerimientos específicos. Los LSPs pueden ser asignados a un mínimo de saltos, reunir ciertos requerimientos para el ancho de banda, requerimientos de apoyo precisos, bypass para los puntos de congestión, tráfico directo fuera del camino dado por el IGP (Interior Gateway Protocol) o simplemente forzar el tráfico a cruzar ciertos enlaces o nodos en la red. (Rossen, 2001, pp.13-15)

1.2.3 Tipos de LSP MPLS

Provee dos opciones para establecer una LSP:

1.2.3.1 Ruteo hop-by-hop

Con el enrutamiento hop by hop, cada LSR independientemente escoge el próximo salto para cada FEC. Esta opción hace uso de un protocolo de enrutamiento ordinario, como OSPF. Además esta opción proporciona algunas de las ventajas de MPLS, incluyendo rápida conmutación de las etiquetas, y tratamiento diferencial de paquetes de diferentes FECs que siguen la misma ruta. Sin embargo, debido al uso limitado del desempeño de la métrica en protocolos de enrutamiento típicos, el enrutamiento hop by hop no soporta fácilmente. (Greossetete, 2001, pp.10-12)

1.2.3.2 Ruteo explícito

El LSR de ingreso especifica la lista de nodos por la cual viaja la trayectoria explícita. Sin embargo, la ruta especificada puede ser no óptima. A lo largo de su trayectoria, los recursos deben ser reservados para asegurar una calidad de servicio para el tráfico de datos. Esto se puede realizar mediante el concepto de ingeniería de tráfico cada LSR independientemente escoge el próximo salto para cada FEC. (Greossetete, 2001, pp.10-12)

1.2.3.3 NHLFE (Next Hop Label Forwarding Entry)

Es una entrada a una tabla de envío en la que se indica la etiqueta del siguiente hop. Por lo tanto, cuando un paquete entra a una red MPLS, se le asigna un determinado FEC. (Greossetete, 2001, pp.10-12)

1.2.3.4 Forwarding equivalence Class

FEC (Forward Equivalent Class): Conjunto de paquetes que tienen los mismos requerimientos para su transporte y son transmitidos por una misma ruta, estos paquetes reciben un mismo trato en MPLS, un FEC está formado por todos los paquetes a los que se le puede aplicar una etiqueta específica y sólo se hace cuando un paquete ingresa a la red. Los FEC se basan en requerimientos de servicio para un conjunto dado de paquetes o simplemente para un prefijo de dirección. Cada LSR construye una tabla que especifica cómo será enviado cada paquete, esta tabla se llama LIB (Label Information

Base). Algunos paquetes pueden pertenecer a los mismos puntos finales pero también pueden pertenecer a diferentes FECs. (Greossetete, 2001, pp.10-12)

El FEC de los paquetes se puede especificar por varios parámetros, tales como:

• Dirección IP destino o Fuente

• ID de Protocolo.

• Etiqueta de Flujo IPv6.

• Puerto Destino o Fuente.

• Punto de código de servicios diferenciados

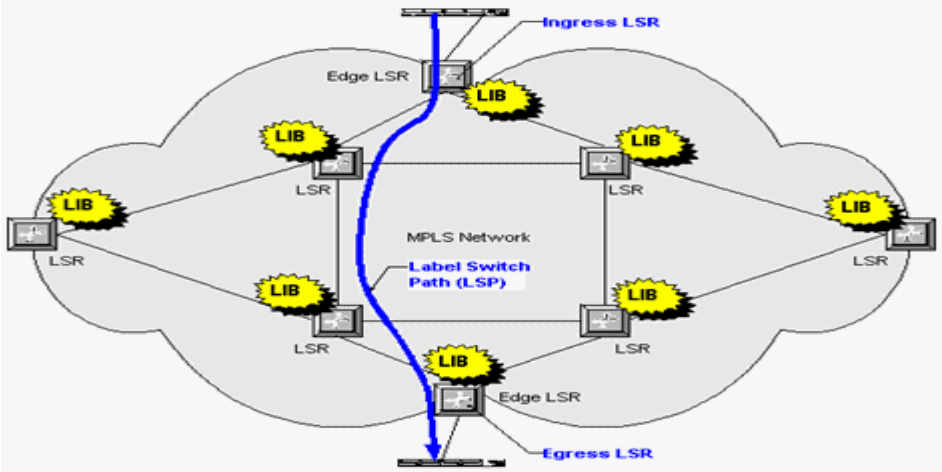


Figura 4- 1 Ejemplos de MPLS

Fuente:(Ingeniería La Salle, 2000)

1.2.4 Etiqueta

Una etiqueta es un campo de 20 bits que establece una correspondencia entre el tráfico y una FEC específica. Esta etiqueta es transportada en la cabecera MPLS de un paquete e identifica el camino por el que debe ser enviado. La asignación de dicha cabecera se realiza en función de la dirección de destino, el tipo de servicio, la pertenencia a una red privada VPN y/o siguiendo otros criterios.

El primer proceso al que se somete un paquete al ingresar a un ruteador MPLS, es el de ser clasificado como una FEC nueva o una ya existente, y es entonces cuando se le asigna una etiqueta al paquete. El valor de las etiquetas se deriva de valores entregados por los protocolos de Capa 2. Para protocolos de capa de enlace de datos (como Frame Relay y ATM), se pueden emplear los identificadores de capa 2 directamente como etiquetas, los DLCIs en el caso de redes frame-relay, o los VPIs/VCIs en

el caso de redes ATM. Entonces el envío de los paquetes se basa en el valor de estas etiquetas. (Galvez, 2002, p.24)

La cabecera genérica MPLS es un campo de 32 bits que se añade a un paquete, entre las cabeceras de nivel 2 y 3, y que define una serie de características y requisitos para su transmisión en una red MPLS.

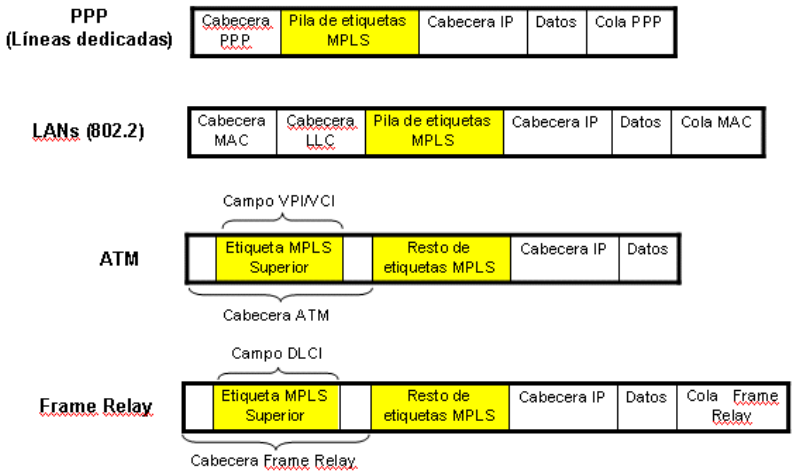


Figura 5- 1: Situación de Etiquetas MPLS

Fuente:(Open SimMPLS, 2000)

1.2.4.1 Estructura de etiquetas

EXP: Este campo consta de 3 bits, se conoce como CoS (Class of Service) y se usa para identificar la clase de servicio.

S (Bottom of Stack): Este campo consta de 1 bit y se usa para indicar si existe una pila de etiquetas (Label Stack) lo cual será indicado con un valor de uno. Si la etiqueta es la única que está en la pila entonces indicará un valor de Cero.

Label Stack (Pila de Etiquetas): MPLS soporta la colocación de varias etiquetas a un sólo paquete. Estas etiquetas se organizan en una pila de etiquetas o Label Stack y su principal aplicación es cuando se puede controlar la trayectoria de un paquete sin que sea necesario especificar los enrutadores intermedios, esto se logra con la realización de túneles por los cuales estos paquetes viajan a través de enrutadores intermedios que permiten avanzar múltiples segmentos, este proceso es conocido como tunneling.

TTL (Time TO Live): Este campo consta de 8 bits e indica el número de nodos recorridos por los que el paquete ha pasado hasta llegar hasta su destino. Este valor es tomado del encabezado IP a la entrada del LSP y a la salida de éste mismo. Las cabeceras MPLS permiten cualquier tecnología o combinación de tecnologías de transporte, con la flexibilidad que esto supone para un proveedor IP a la hora de extender su red. Con las etiquetas se pueden realizar dos tipos de operaciones: Una es el cambio del valor de la etiqueta en cada uno de los nodos (Label Swap) y la otra es el cambio de varias etiquetas que identifican el mismo FEC por una única (Label Merging). (Galvez, 2002, p.24)

1.2.5 Pila de etiquetas (LABEL STACK)

Uno de los aspectos más poderosos de MPLS es la pila o acumulamiento de etiquetas. Un paquete etiquetado puede llevar muchas etiquetas, organizado como una pila LIFO de etiquetas (último en entrar primero en salir). El procesamiento está siempre basado en la etiqueta de la cima. En cualquier LSR, la etiqueta puede ser añadida a la pila (operación push) o removida de la pila (operación pop). El apilamiento de etiquetas permite la agregación de LSPs en un solo LSP para una porción de la ruta a través de una red, creando un túnel.

Al principio del túnel, un LSR asigna la misma etiqueta a los paquetes de un número de LSPs colocando la etiqueta sobre la pila de cada paquete. Al final del túnel, otro LSR extrae el elemento de la cima de la pila de la etiqueta, mostrando la etiqueta interna. Esto es similar a ATM que tiene un nivel de pila (canales virtuales dentro de caminos virtuales), pero MPLS soporta una pila ilimitada. La pila de etiquetas proporciona una considerable flexibilidad en la transmisión de la información. Este proceso está basado en la etiqueta de más alta numeración, sin contemplar la posibilidad de que algún número de otra etiqueta haya sido anteriormente la más alta o que otro número de alguna etiqueta haya estado por debajo de esa. (Gallear, 2003, pp.19-20)

Un paquete sin etiquetar puede pensarse como un paquete cuya pila de etiqueta está vacía cuya pila de etiqueta tiene una profundidad O (depth). Si la pila de la etiqueta de un paquete es de profundidad m, se referirá a la etiqueta en el fondo de la pila como la etiqueta de nivel 1, a la etiqueta sobre él (si existe) como la etiqueta de nivel 2 y a la etiqueta en la cima de la pila como la etiqueta de nivel m. La utilidad de etiquetas en pila llega a ser muy buena cuando se introduce la noción de túnel LSP y de jerarquía en MPLS.

En un modelo más general, MPLS soporta la colocación de múltiples etiquetas a un solo paquete; en este caso, se soporta un diseño de ruteo jerárquico. Estas etiquetas se organizan en una pila o "stack"

con una forma last-in, first-out (LIFO), y forma la llamada pila de etiquetas o label stack. El principal empleo de la pila de etiquetas se tiene cuando se emplea una operación MPLS llamada Tunneling. (Gallear, 2003, pp.19-20)

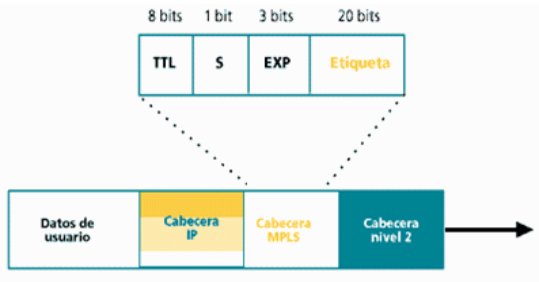


Figura 6- 1 Etiqueta MPLS genérica

Fuente:(Ingeniería La Salle, 2000)

1.2.6 Nodos mpls

Un nodo MPLS es un dispositivo de interconexión que soporta MPLS. Tiene conocimiento de los protocolos de control MPLS, opera en uno o más protocolos de enrutamiento de capa 3, y es capaz de reenviar paquetes en base a etiquetas. Opcionalmente, puede reenviar paquetes capa 3 nativos. Los nodos MPLS son llamados LSR (Label Switching Router). Existen diferentes tipos de nodos MPLS: Nodo de tránsito (Transit Node): Recibe el PDU y usa la cabecera MPLS para tomar las decisiones de reenvío, asimismo realiza intercambio de etiquetas. También es llamado LSR interior, o LSR de Core.

Nodo de borde (Edge Node): Conecta un dominio MPLS con un nodo fuera del dominio, ya sea porque no soporta MPLS, y/o porque está en un dominio diferente. Pueden haber dos tipos, de acuerdo al rol que adopten en un momento dado: o Nodo de egreso (Egress Node): maneja el tráfico que sale del dominio MPLS. O Nodo de ingreso (Ingress Node): maneja el tráfico que entra en el dominio MPLS. (Affarel, 2006, p. 17)

1.2.7 Distribución de etiquetas

En cuanto al proceso de distribución de etiquetas, se plantean conceptos que indican la dirección en que éste ocurre: upstream y downstrem. Por ejemplo: tenemos dos LSRs, R1 y R2, y estos concuerdan

en atar la etiqueta L a la FEC Z, para paquetes mandados de R1 a R2. Entonces se dice que con respecto a esta unión, R1 es el LSR upstream y R2 es el LSR downstream. . (Affarel, 2006, pp. 18-20)

Cuando se dice que un nodo es upstream y otro es downstream con respecto a una unión, significa "únicamente" que etiqueta en particular representa a una FEC en paquetes que viajan del nodo upstream al nodo downstream (significancia local de la etiqueta). Esto "no" implica que todos los paquetes de tal FEC tengan que ser necesariamente ruteados del nodo upstream al nodo downstream.

La arquitectura MPLS no reconoce solamente a un método de señalización para la distribución de etiquetas. Protocolos existentes han sido extendidos, de manera que la información de etiquetas pueda ser "cargada a cuestas" dentro de los contenidos del protocolo (por ejemplo BGP, o túneles RSVP). El IETF ha definido en paralelo con la arquitectura MPLS, un nuevo protocolo conocido como el Protocolo de Distribución de Etiquetas (LDP), para un explícito manejo y señalización del espacio de etiqueta. (Affarel, 2006, pp. 18-20)

También se han definido extensiones al protocolo LDP base, para soportar ruteo explícito basado en requerimientos QoS y CoS; estas extensiones se concentran en el protocolo Constraint-Based Label Distribution Protocol (CR-LDP). Los principales protocolos existentes y sus principales características son LDP, RSVP, CR-LDP, Protocol-Independent Multicast (PIM) y BGP (en el caso de VPNs).Aunque no se especifica un protocolo específico para la distribución de las etiquetas, sí se definen los modos de distribución y retención de etiquetas dentro del funcionamiento de MPLS.

Downstream On Demand (Tráfico de Bajada bajo Demanda): Permite que un enrutador upstream (Enrutador que envía paquetes) haga una petición directa de una etiqueta para un determinado grupo de paquetes (FEC) al LSR Downstream, el cual es el siguiente salto en el camino.

Unsolicited Downstream (Tráfico de Bajada no Solicitado): Permite que un LSR Downstream asigne una etiqueta sin necesidad de recibir peticiones con anterioridad. (Affarel, 2006, pp. 18-20)

Unsolicited Downstream (Tráfico de Bajada no Solicitado): Permite que un LSR Downstream asigne una etiqueta sin necesidad de recibir peticiones con anterioridad. Una vez el LSR ha recibido la asignación correspondiente a un determinado FEC éste podría conservar o desechar dicha asignación, si el LSR reconoce que dicha asignación ha dejado de ser válida entonces la desecha, esta condición se conoce como Modo de Retención Conservador de Etiquetas.

Además, para no perder el vínculo entre el FEC y la etiqueta se debe repetir el procedimiento de asignación tantas veces como sea necesario, con la ventaja de sólo asignar las etiquetas que realmente están en uso. Si el LSR ha recibido una asignación la mantiene indefinidamente, esta condición se conoce como Modo de Retención Liberal de Etiquetas, la desventaja de esta condición es que el consumo de etiquetas es excesivo aunque el procedimiento para mantener la relación entre el FEC y la etiqueta ya no es necesario, pero tiene como ventaja que permite una adaptación más rápida a los cambios en la topología y permite el envío de tráfico a diferentes LSP en caso de cambio. (Affarel, 2006, pp. 18-20)

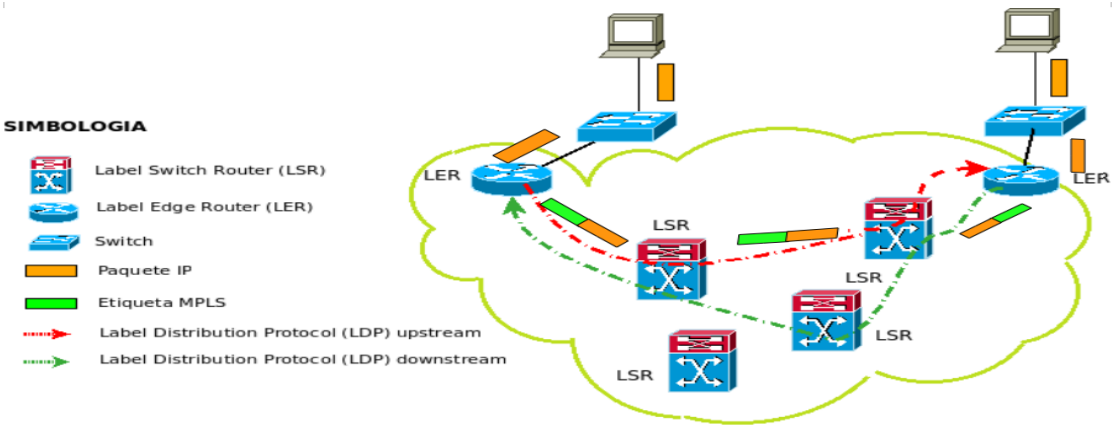


Figura 7- 1 Esquema de distribución

Fuente:(Ingeniería La Salle, 2000)

1.2.7.1 Control de distribución de etiquetas

Existen dos modos para el Control de Distribución de Etiquetas entre dos LSR pares:

Control Independiente: Este tipo de control se da cuando un LSR reconoce una FEC y decide unir una etiqueta a esta FEC, es decir significa que cada nodo toma la decisión de cómo tratar a cada paquete que pasa por éste y distribuir esta unión a los LSR pares.

Control Ordenado: Este tipo de control se da cuando un LER une una etiqueta a una FEC, el cual es responsable de la asignación y distribución de etiquetas. (Beijnum, 2012, p. 28)

1.2.7.2 Protocolos para distribución de etiquetas.

El IETF nombra diferentes protocolos de distribución de etiquetas que se crean con el propósito de mantener informados a los LSR de las asignaciones de etiquetas a las FECs, entre los protocolos tenemos RSVP, CR-LDP y LDP (el cual es el más recomendado por el IETF). En MPLS no se impone ningún protocolo en particular para la distribución de etiquetas.

• Antes de que el tráfico empiece a fluir, los LSRs toman decisiones para unir una etiqueta a una FEC, y construir sus tablas.
• Con LDP, los routers downstream inician la distribución de etiquetas y de las uniones etiqueta/FEC.
•También LDP realiza las negociaciones de las características relacionadas con tráfico y de las capacidades MPLS.
• Se usa un protocolo de transporte ordenado y confiable como protocolo de señalización. El LDP usa TCP. (Affarel, 2006, pp. 18-20)

1.2.7.3 Encapsulación de Etiquetas

La pila de etiquetas aparece después de la cabecera de capa enlace, pero antes de la cabecera de capa red. El paquete de capa red sigue inmediatamente a la entrada de la pila de etiquetas que tiene el bit S puesto a 1. En una trama de capa enlace como para la pila de etiquetas aparece entre la cabecera IP y la cabecera de capa enlace. Para una trama IEEE 802 la pila de etiquetas aparece entre la cabecera IP y la cabecera LLC (Lógica! Link Control).

Si MPLS es usada sobre una red de servicios orientada a conexión, puede asumirse un enfoque ligeramente diferente. Para celdas ATM, el valor de la etiqueta que se encuentra en la cima de la pila es colocada en el campo del identificador de camino y canal virtual (VPIA/CI) en la cabecera de la celda ATM. La etiqueta más alta permanece en la cima de la pila, la cual es insertada entre la cabecera de la celda y la cabecera IP. Colocando el valor de la etiqueta en la cabecera de la celda ATM facilita la conmutación por un switch ATM. (Evans, 2008, p. 41)

1.2.7.4 Uniones a etiquetas

Las etiquetas son enlazadas a una FEC como resultado de algún evento o política que indica la necesidad por dicha etiqueta. Estos eventos de unión pueden ser divididos en dos categorías:

Uniones Data-Driven.- ocurre cuando el tráfico comienza a fluir, éste es sometido al LSR y es reconocido como un candidato a label switching (usa la recepción de un paquete para disparar el proceso de asignación y distribución de etiquetas). Las uniones a etiquetas son establecidas sólo cuando son necesitadas y son asignadas a flujos individuales de tráfico IP, y no a paquetes individuales.

Uniones Control-Driven.- se establecen como resultado de la actividad del plano de control y son independientes del flujo de datos. Las uniones pueden ser establecidas como respuesta a actualizaciones de ruteo (usa procesamiento de protocolos de ruteo como OSPF y BGP), o por la recepción de mensajes RSVP (usa procesamiento de control de tráfico basado en peticiones). (Evans, 2008, p. 40)

1.2.8 Clasificación de etiquetas

Las etiquetas utilizadas por un LSR para unir el FEC y la etiqueta se clasifican en dos formas:

Por Plataforma: Los valores de las etiquetas son proporcionados por una sola fuente, es decir, los valores de etiquetas son los mismos dentro de un LSR lo que quiere decir que por cada interfaz hay una etiqueta y no existe la posibilidad que dos etiquetas distribuidas en interfaces diferentes se repitan.

Por Interfaz: Las etiquetas son suministradas por diferentes fuentes, es decir que los valores de etiqueta son diferentes dentro de un LSR. Estos valores de etiqueta son asignados a diferentes interfaces y pueden existir una o más interfaces con un mismo valor de etiqueta. (Evans, 2008, p. 42)

1.2.9 Mecanismos de señalización

Solicitud de Etiqueta: Esta solicitud es realizada por un LSP el cual le solicita a su vecino Downstream (en la ruta de bajada) una etiqueta para que sea asignada a una FEC, esto lo realizan todos los LSRs durante la ruta hasta llegar al destino final, es decir, hasta el LER de borde.

Mapeo de Etiqueta: El mapeo surge del envío de la etiqueta que el LSR Downstream envíe como respuesta a la solicitud realizada por el LSR Upstream utilizando el mecanismo de mapeo. (Evans, 2008, p. 44)

1.3 Funcionamiento global

La tecnología MPLS se despliega en el núcleo de la red del proveedor de servicios, lo que le proporciona a éste un mayor control sobre la calidad del servicio, la ingeniería de tráfico y la utilización del ancho de banda, y a la vez que reduce los requisitos a los equipos de comunicación de los clientes que se conectan a un servicio sobre MPLS. (Rosen, 2007: 70-74)

Como indica su nombre, una red MPLS puede transportar múltiples protocolos distintos y de forma simultánea, entre ellos tramas Ethernet, realizando conexiones Ethernet sobre largas distancias. El modo de funcionamiento de MPLS es algo muy similar a las redes de capa 2 (ATM o Frame Relay), con la diferencia que MPLS lo que hace es asignar etiquetas a los paquetes que viajan a través de la red, donde cada paquete contiene una etiqueta que tiene la tarea de informar a cada nodo la forma de procesar y transportar los datos.

La diferencia básica entre MPLS y las tecnologías WAN tradicionales es la forma como son asignadas las etiquetas y la capacidad de transportar una pila de etiquetas junto con el paquete, para el desarrollo de nuevas aplicaciones como Ingeniería de tráfico, rápido enrutamiento en caso de fallas de enlaces o nodos, entre otras.

Se refleja las diversas funciones en cada uno de los elementos que integran la red MPLS. Es importante destacar que en el borde de la nube MPLS tenemos una red convencional de routers IP, el núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de routers a una distancia de un solo salto. Funcionalmente es como si estuvieran unidos todos en una topología mallada (directamente o por PVC ATM), ahora esa unión a un solo salto se realiza por MPLS mediante los correspondientes LSPs (puede haber más de uno para cada par de routers).
La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y que no se pierde la visibilidad sobre los paquetes IP. Todo ello abre enormes posibilidades a la hora de mejorar el rendimiento de las redes y de soportar nuevas aplicaciones de usuario. (Beijnum, 2012, pp. 70-74)

Funcionamiento de una red MPLS se basa en cinco (5) pasos:

1. Construcción de tablas de encaminamiento.
2. Creación de rutas LSPs.
3. Construcción de LSPs.
4. Inserción de etiquetas.
5. Envío de paquetes.

1.3.1 Construcción de tablas de encaminamiento.

Esta creación de etiquetas inicia en el momento en que los LSR toman la decisión de unir una etiqueta a un FEC. Con el protocolo de Distribución de Etiquetas (LDP) los enrutadores downstream son los que inician la distribución de dichas etiquetas y la asignación de las mismas a la FEC, adicional a esto los LDP se encargan de establecer características que tiene que ver con el tráfico y la capacidad de MPLS.

El protocolo de encaminamiento envía el paquete y enseguida el protocolo RSVP hace las reservas necesarias para obtener un buen servicio a lo largo de la ruta, en pocas palabras el protocolo de encaminamiento indica para dónde va el paquete y el protocolo RSVP determina la QoS con que éste viaja, estas reservas son necesarias en cada uno de los nodos. Éste es un protocolo simplex, es decir que trabaja en un sólo sentido y se pueden hacer como receptor o como emisor. Existen dos tipos de mensajes en RSVP: (Lloyd, 2001: 41)

Mensajes Path: Estos mensajes son generados por los emisores y son los que se encargan de describir el formato de los paquetes que el emisor enviará, además de determinar la dirección IP y su ruta de manera opcional. Este mensaje es usado por los enrutadores para definir la ruta de una nueva sesión.

Mensaje Resv: Estos mensajes son generados por los receptores y son usados cuando se desea hacer una reserva de recursos y por lo general esta reserva se aplica en todos los nodos por los que el paquete viaja a través de la red. Para la asignación de etiquetas en MPLS a este protocolo se aplican nuevos elementos como son los objetos, formatos de paquetes y procedimientos para establecer túneles LSP, los cuales permiten el transporte de flujo de datos por debajo de los procedimientos básicos de enrutamiento IP.

Para lograr establecer un túnel LSP es necesario utilizar un modo de señalización llamado Downstream on Demand para la distribución de etiquetas MPLS. La creación de un túnel LSP inicia por el LSE de entrada en el momento que se asocia una FEC y una etiqueta.

Para facilitar la gestión de tráfico en el dominio MPLS es necesario agregar nuevos objetos llamados EXPLICIT_ROUTE en los mensajes Path, el cual agrupa la cantidad de nodos de manera ordenada que forma la ruta explícita que seguirán los datos, para el funcionamiento de este objeto es fundamental que el dominio MPLS soporte el encaminamiento explicito (EXPLICIT ROUTING).

También es necesario incrementar el mensaje Resv debido a que la asignación de etiquetas se hace desde el nodo final al nodo origen, es decir, en sentido contrario al flujo de datos y a esto se adiciona un nuevo objeto (Label) el cual transporta la nueva información requerida para el buen funcionamiento del protocolo. (Jarrin, 2001, pp.87-89)

1.3.2 Creación de rutas LSP's.

Cuando un LSR recibe las asignaciones de etiquetas crea entradas para la base de datos de información de etiquetas (LIB), la cual especifica el mapeo entre una etiqueta y una FEC.

Las tablas de enrutamiento se construyen usando los algoritmos implementados en el sistema, ya sean como OSPF (Open Shortest Path First), IS-IS o RIP (Routing Information Protocol) y exteriores como los BGP (Border Gateway Protocol) y actualización del EGP (External Gateway Protocol) que intercambiarán información con los enrutadores vecinos que estén conectados a la misma red o por un enlace punto a punto y con los vecinos exteriores que serán los conectados a sistemas independientes diferentes.

Para la construcción de las tablas cada dispositivo de la red MPLS consulta las tablas de etiquetas y dependiendo de la etiqueta y el puerto de entrada del paquete se decide la interfaz de salida de éste y la etiqueta a sustituir, en el caso de los enrutadores de borde, LER, los campos de etiqueta de entrada y salida se encontrarán en cero, ya sea que se esté recibiendo un paquete desde un dispositivo fuera de la red MPLS o se esté enviando a un dispositivo fuera de la red MPLS. (Rosen, 2007: 70-74)

1.3.3 Construcción de LSP's

La construcción de LSP's se realiza utilizando la información de las tablas de intercambio de etiquetas entre los LSR's adyacentes. Esta distribución se hace mediante el protocolo LDP el cual ha sido definido específicamente para MPLS, aunque RSVP (Resource Reservation Protocol) o CR-LDP (Constraint Based-Label Protocol Distribution) también puede ser una opción. Los LSP se pueden establecer de las siguientes maneras:

Routing hop by hop: Este tipo de enrutamiento se caracteriza porque cada uno de los LSR's selecciona de forma independiente el siguiente hop para una FEC determinada.

Explicit Routing – LSP (ER-LSP): Este tipo de ruteo a diferencia del anterior es definido desde la fuente por el propio operador de la red. Sin embargo, la ruta específica puede ser no óptima, haciéndose necesario que a lo largo de la trayectoria, los recursos deban ser reservados para asegurar una calidad de servicio para el tráfico de datos. (Rekhter, 2006, p. 71)

1.3.4 Inserción de etiquetas.

El LER de ingreso a la tabla LIB para encontrar el siguiente salto, hace una petición de una etiqueta para una FEC en particular, de esta forma cada paquete que pasa por un LER de entrada y se dispone a utilizar el dominio MPLS recibe una etiqueta y es enviado al núcleo de la red por la ruta LSP definida, dicha etiqueta es insertada en un encabezado de Capa 2, junto con el paquete.

De este modo los enrutadores que reciben el paquete examinan la etiqueta y basándose en la información que ésta contiene determina el siguiente salto, una vez el paquete ha sido etiquetado el resto del viaje se hace mediante la conmutación de etiquetas, finalmente cuando el paquete llega al LER de egreso, la etiqueta es removida y el paquete es entregado a su destino final. (Rekhter, 2006, p. 73)

1.3.5 Envío de paquetes.

Existe una trayectoria que ha sido creada para que los paquetes viajen de LER1 a LER2, a través de LSR1 LSR2 y LSR4, donde es posible que el LER1 no tenga ninguna etiqueta disponible, ya que es la primera solicitud de enrutamiento que se realiza, así que lo que tiene que hacer es utilizar el

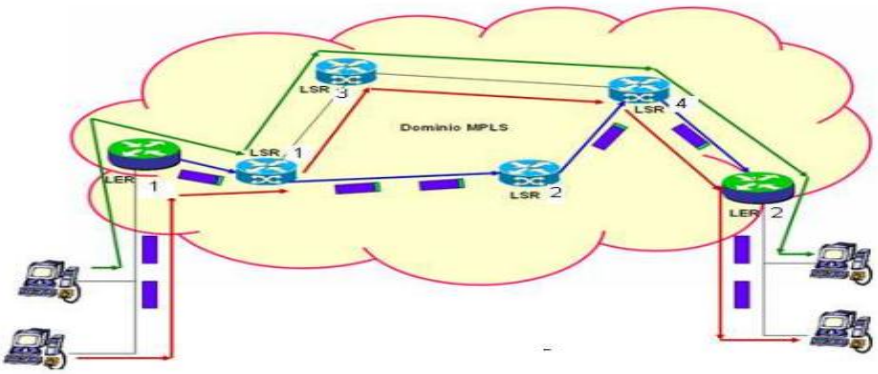


Figura 8- 1 Envió de paquetes MPLS
Fuente:(Ingeniería La Salle, 2000)

Algoritmo Longest Address Match, el cual especifica que el LSR1 es su siguiente salto. LER1 inicia entonces el requerimiento de etiqueta hacia LSR1 y es así como el requerimiento se propaga por la trayectoria en dirección de LER2.

El LER2 que funciona como administrador de etiquetas, distribuye las etiquetas en dirección Upstream, pasando por cada nodo de la trayectoria, es así como el protocolo LDP realiza el establecimiento de trayectoria. Entonces el LER1 inserta la etiqueta y envía el paquete hacia el LSR1, donde éste lo envía hacia otro LSR y así sucesivamente realizando el intercambio de etiquetas con cada enrutador que se encuentra en el camino, hasta que el paquete llegue al LER2 donde se retira la etiqueta ya que el paquete sale del dominio MPLS y es entregado a su destino. (Evans, 2008, p.47)

1.4 Aplicaciones de mpls

Las aplicaciones principales de MPLS son las siguientes:

- Encaminamiento explícito e ingeniería de tráfico.
- Soporte a las CoS

1.4.1 La ingeniería de tráfico

Es el proceso de mapear la demanda de tráfico sobre la topología de la red. Se refiere a la habilidad de definir rutas dinámicamente y planear la asignación de recursos con base en la demanda, así como optimizar el uso de la red. El RFC 2702, 'MPLS Traffic Engineering (TE)' establece que la ingeniería de tráfico concierne a la optimización de la performance de una red e involucra diversas áreas:

Mediciones de tráfico, Modelado de tráfico y redes, Control del tráfico en Internet, Evaluación de performance. (Márquez, 2005, pp. 24-32)

Uno de los mayores problemas de las redes IP actuales es la dificultad de ajustar el tráfico IP para hacer un mejor uso del ancho de banda, así como mandar flujos específicos por caminos específicos. En las redes IP convencionales, los paquetes suelen seguir el camino más corto, política que siguen los protocolos de encaminamiento interior. Esto suele provocar que algunos enlaces se saturen mientras otros están infrautilizados. Dicho problema se ha venido resolviendo añadiendo más capacidad a los enlaces. (Márquez, 2005, pp. 24-32)

Una ventaja práctica de la aplicación sistemática de los conceptos de Ingeniería de Tráfico a las redes operacionales es que ayuda a identificar y estructurar las metas y prioridades en términos de mejora de la calidad de servicio dado a los usuarios finales de los servicios de la red. También la aplicación de los conceptos de Ingeniería de Tráfico ayuda en la medición y análisis del cumplimiento de éstas metas. (Márquez, 2005, pp. 24-32)

La ingeniería de tráfico se subdivide en dos ramas principalmente diferenciadas por sus objetivos:
Orientada a tráfico: ésta rama tiene como prioridad la mejora de los indicadores relativos al transporte de datos, como por ejemplo: minimizar la pérdida de paquetes, minimizar el retardo, maximizar el Throughput, obtener distintos niveles de acuerdo para brindar calidad de servicio, etc.

Orientada a recursos: ésta rama se plantea como objetivo, la optimización de la utilización de los recursos de la red, de manera que, no se saturen partes de la red mientras otras permanecen subutilizadas, tomando principalmente el ancho de banda como recurso a optimizar.

En general la TE comprende la aplicación de la tecnología y de los principios científicos a la medición, modelado, caracterización y control del tráfico en Internet. Los objetivos más importantes asociados con la TE pueden ser clasificados así:
Objetivos de funcionamiento orientados al Tráfico.- Comprende los aspectos que mejoran la calidad de servicio de los flujos de tráfico. En redes Best effort, estos parámetros de desempeño vienen dados por minimización del retardo, minimización de pérdidas, maximización del Throughput, entre otros.

Objetivos de funcionamiento orientados a los Recursos.- Se refiere a los aspectos que brinden una optimización en el uso de los recursos. Adicionalmente los mecanismos de la Ingeniería de Tráfico están clasificados en dos tipos básicos, acorde a la escala de aplicación que se quiere abarcar.
TE Dependiente de Tiempo.- En este caso, los algoritmos de control de tráfico son utilizados para optimizar el uso de los recursos de la red en respuesta a variaciones de tráfico medidos en una escala de tiempo muy larga. (Márquez, 2005, pp. 24-32)

TE Dependiente del Estado.- los algoritmos o mecanismos de control de tráfico se deben adaptar a los cambios de estado que sufre la red en forma casi instantánea. (Márquez, 2005, pp. 24-32)

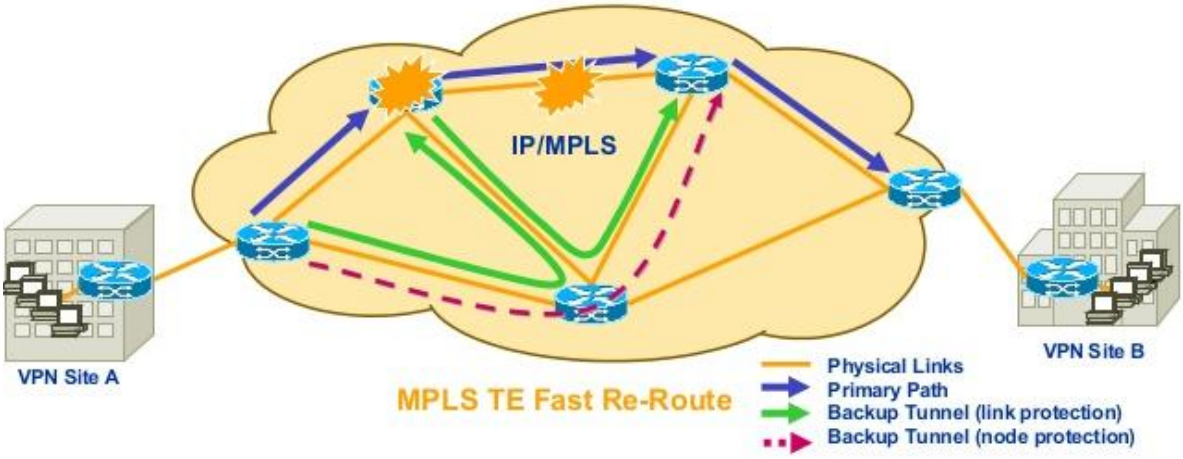


Figura 9- 1 Diagrama Ingeniera en Tráfico
Fuente:(Ingeniería La Salle, 2000)

1.4.2 Aplicaciones de ingeniería de tráfico

La ingeniería de tráfico tiene muchas aplicaciones, por ejemplo podría utilizarse ingeniería de tráfico cuando:

- Se presente algún problema con los enlaces ya que esto hace que un LSP no funcione, en este momento se puede habilitar un camino o varios alternativos para evitar que la comunicación se interrumpa.
- Los protocolos de encaminamiento que eligen el camino más corto de los posibles pueden provocar que, pese a existir caminos alternativos, sólo se utilice uno y por tanto se sature, con ingeniería de tráfico se puede desviar parte de este tráfico por otro camino posible.

En redes tradicionales Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente. En casos de congestión de algunos enlaces, el problema se resolvía a base de añadir más capacidad a los enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta.(Marquez,2005,p 24)

1.4.3 Balanceo de carga

El Balanceo de Carga es un aspecto clave en los esquemas de TE aplicados a las redes IP. Es utilizado como un mecanismo para la asignación adaptativa de tráfico a los enlaces de salida disponibles, dicha asignación se realiza de acuerdo al estado actual de la red; el conocimiento de dicho estado puede estar basado en la utilización, retardo del paquete, pérdida del paquete, etc.

Por tal razón, la eficiencia de cualquier mecanismo de balanceo de carga depende crucialmente del proceso de medidas del tráfico que ingresa a la red y se requiere una gran habilidad para controlarlo de forma precisa, dada la naturaleza dinámica del mismo.

Por regla general, las decisiones y operaciones relacionadas con el balanceo de carga se realizan en los nodos de ingreso, quienes tienen, un mejor conocimiento del tráfico que se inyecta a la red. Los nodos intermedios se encargan de realizar funciones de re-envío y en ciertos casos de recolectar información sobre el tráfico en la red y enviarla al nodo de ingreso.

El Balanceo de Carga (Load Balancing), también conocido como Compartición de Carga (Load Sharing) o División de Tráfico (Traffic Splitting) es un mecanismo importante para mejorar el funcionamiento (en aspectos de caudal, retardo, jitter y pérdidas) y las prestaciones de la red.
(Marquez, 2005, p 24)

1.5 Calidad de servicio

Se conoce como Calidad de Servicio (QoS) los efectos colectivos o globales de las prestaciones de uno o múltiples servicios, en estos casos aplicaciones diversas, los cuales determinan el grado de satisfacción de un usuario con respecto al servicio o servicios contratados por una o varias entidades. Puede entenderse además que es el conjunto de requisitos del servicio que debe cumplir la red en el

transporte de un flujo.

Cuando la Internet surgió no se necesitaba gran demanda de velocidad, Ingeniería de Tráfico, prioridades, diferenciación del tráfico, entre otro; solo se requería aplicaciones en las que solo importaba la información, en forma de paquetes, llegase a su destino de manera segura y fiable.
El stack TCP/IP cubrió perfectamente las demandas que se necesitaban de envío de paquetes así como el control de flujo necesario.

Con el primer crecimiento de la Internet, se necesitó aplicar Ingeniería de Red, es decir, los enlaces más usados debían ser mejorados e incrementar su capacidad de transferencia y así poder adecuarlos a la nueva demanda. Arquitecturas como IP over Frame Relay y IPoverATM, de las cuales la más usada es la última por poseer la capacidad de transferencia que puede llegar a un Gigabit de velocidad y fueron usadas para incrementar las capacidades los requerimientos de aquel entonces.

Gracias a la convergencia de los servicios en tiempo real y al creciente número de usuarios, los ISPs no podían seguir aplicando Ingeniería de Red ya que no resultaba eficiente y menos conveniente invertir grandes cantidades para incrementar la capacidad de un solo enlace mientras otros de menor capacidad eran subutilizados. (Kodialam, 2009, pp27-38)

La vía para poder utilizar de forma óptima la red era aplicando Ingeniería de Tráfico .Las nuevas aplicaciones no requieren solamente que el tráfico llegue a su destino; dependiendo de la aplicación se necesitará retardo asegurado, ancho de banda asegurado, un jitter mínimo, probabilidad de pérdida determinada, entre otros.

Los protocolos de enrutamiento tradicionales tales como RIP, OSPFv2, IS-IS no son capaces de detectar los picos de tráfico que se dan en las redes, la gestión de colas no beneficia a los tráficos sensibles a los retardos y a su variabilidad. Arquitecturas que sean capaces de proporcionar la Calidad de Servicio necesaria para las aplicaciones así como lo requerido en el LSA son propuestos en base a nuevos protocolos de Internet de la Nueva Generación como IPv6, MPLS, RSVP, entre otros.

La ITU-T propone arquitecturas en las cuales se cumplan los requerimientos de QoS: Capacidad de Transferencia con Anchura de banda Dedicada DBW (Dedicated Bandwidth), Capacidad de Transferencia con anchura de banda Estadística SBW (statistical bandwidth), y finalmente Capacidad de transferencia de tipo mejor esfuerzo Best Effort y las recomendaciones dependiendo del tipo de

tráfico que quiere cursar en la red y los parámetros que se deberían cumplir. (Kodialam, 2009, pp27-38)

Por otro lado la IETF (Internet Engineering Task Force) ha propuesto nuevas arquitecturas que podrían dar solución a los requerimientos de Calidad de Servicios actuales gracias al uso de nuevas tecnologías tales como IPv6. Estas arquitecturas: Arquitectura de Servicios Diferenciados DiffServ, Arquitectura de Servicios Integrados IntServ y además se encuentra la arquitectura actual bajo el esquema Best Effort.

Los siguientes parámetros son comúnmente utilizados para describir requisitos de QoS:

Ancho de Banda Mínimo: Es la mínima cantidad del ancho de banda requerida por el flujo de una aplicación. Es necesario especificar el intervalo de tiempo para la medición del ancho de banda ya que diferentes intervalos de medición pueden producir diferentes resultados.

Retardo (delay): El retardo requerido puede ser especificado como el promedio de los retardos (Retardo Medio) o por el retardo del peor caso. El retardo que un paquete experimenta tiene tres componentes: retardo de propagación, retardo de transmisión, y retardo de procesamiento. El retardo de propagación es limitado por la velocidad de la luz, y al mismo tiempo es una función de la distancia. El retardo de transmisión es el tiempo que tarda en enviarse un paquete en un enlace y depende de la longitud del paquete y de la velocidad del enlace; finalmente, el retardo de procesamiento es el tiempo de espera que experimenta un paquete en las colas de los Encaminadores.

Variación de Retardo (Delay Jitter): Este parámetro especifica la máxima diferencia entre el más largo y el más corto retardo que un paquete experimenta. En cualquier caso, la variación de retardo no debería ser más larga que el retardo del peor caso ni tampoco que el retardo de procesamiento.

Tasa de Pérdidas (Loss Rate): Es el cociente resultante entre los paquetes perdidos y el total de los paquetes transmitidos. La pérdida de paquetes en una Internet se debe usualmente a la congestión, y tales pérdidas pueden ser prevenidas mediante la asignación de suficiente ancho de banda y suficiente almacenamiento intermedio (Buffers) para el flujo de tráfico. A la capacidad de una red para asegurar una cantidad de recursos y diferenciar servicios se le conoce como Calidad de Servicio (QoS, Quality of Service). Para que Internet tenga esta capacidad se han desarrollado dos soluciones básicas con diferentes formas. (Kodialam, 2009, pp27-30)

1.5.1 Calidad de servicio (QoS) y clases de servicios (CoS)

Una de las características clave de MPLS, comparado con redes tradicionales como Frame Relay y ATM, es que está diseñado para proveer servicios garantizados. Es decir, que según los requisitos de los usuarios, permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de video y voz interactiva. (Redford, 2004: 35)

QoS y clases de servicios factores fundamentales de esta tecnología pueden ser implementados a través de ingeniería de tráfico. Esta capacidad permite proveer a los distintos usuarios; un servicio de nivel estable (Service level Agreements, SLAs) en aspectos como: ancho de banda, tiempo de demora, y variación del mismo. Generando un valor agregado a los prestadores de servicios y proponiendo a estos últimos la migración hacia estas redes. (Pico, 2009, p.24)

1.5.2 Parámetros de calidad de servicio

La ITU-T define parámetros de calidad de servicio con los cuales se basa para definir los diferentes requerimientos de las aplicaciones así como de los clientes hacen a la red del proveedor a través del LSA. Estos parámetros varían de tráfico en tráfico y de cliente en cliente, según los requerimientos y los aspectos técnicos de la red. Los parámetros que se mencionan se pueden utilizar para los diferentes tipos de especificaciones para la evaluación de la calidad de funcionamiento de la red en lo referente a rendimiento de velocidad, exactitud del envío, seguridad en el funcionamiento y disponibilidad de la transmisión de los diferentes paquetes IP a nivel mundial ya sea de extremo a extremo, punto a punto y a tramos de la red.

Retardo de transferencia de paquetes IP (IPTD). El retardo que sufre un paquete IP cuando es transmitido entre dos puntos de referencia cualesquiera. Se entiende que los puntos de referencia son puntos de extremo a extremo o puntos que se encuentran dentro de una red.

Retardo medio en la transferencia de los paquetes IP. Este valor representa a la media aritmética de los diferentes retrasos que pueden sufrir los paquetes IP al ser transmitidos en la red. Recuérdese que los valores de retardo no son fijos ya que estos varían por lo que la media nos puede dar una idea cercana en algunos casos a lo que se podría esperar en el rendimiento de la red.

Varianza del retardo de los paquetes de información (IPDV). Este parámetro se refiere al jitter o variación del retardo. Esta variación difícilmente sigue algún comportamiento fijo o que se pueda predecir, es decir, es aleatorio el valor que se tiene de muestra en muestra. Tráficos sensibles al retardo y a la variación de este dependen mucho de este parámetro para su funcionamiento.

Tasa de errores en los paquetes IP (IPER). Se refiere a los paquetes erróneos que se obtiene en una transmisión total de paquetes. Las posibles fuentes de errores pueden venir desde la codificación en el trasmisor o fuente de tráfico hasta en la decodificación de la información en el receptor.
Tasa de pérdida de paquetes IP (IPLR). Porcentaje de paquetes descartados de un total que han sido trasmitidos. Estas pérdidas se pueden dar por diversos motivos tales como congestión en las colas de los nodos, tiempo de vida (TTL en IPv4, HL en IPv6) prefijado ha expirado, algún nodo que ha fallado en la trasmisión, entre otros.

Tasa de paquetes IP espurios (SPR). Cuantifica el total de paquetes espurios detectados en el punto de medición de egreso en un intervalo de tiempo dividido por la duración del intervalo. Estos paquetes se generan por errores en la capa física como por errores en los nodos intermedios.

Porcentaje de indisponibilidad del servicio IP (PIU). Este factor indica el porcentaje del tiempo del servicio programado total que se clasifica como período indisponible utilizando la función de disponibilidad del servicio. La función de disponibilidad de un servicio IP se basa en un umbral de la característica IPLR. (Kodialam, 2009, p.32)

1.5.3 Beneficios principales de QoS

QoS trabaja a lo largo de la red y se encarga de asignar recursos a las aplicaciones que lo requieran, dichos recursos se refieren principalmente al ancho de banda. Para asignar estos recursos QoS se basa en prioridades, algunas aplicaciones podrán tener más prioridades que otras, sin embargo se garantiza que todas las aplicaciones tendrán los recursos necesarios para completar sus transacciones en un periodo de tiempo aceptable.

En resumen QoS otorga mayor control a los administradores sobre sus redes, mejora la interacción del usuario con el sistema y reduce costos al asignar recursos con mayor eficiencia (bandwidth). Mejora el control sobre la latencia (Latency y jitter) para asegurar la capacidad de transmisión de voz sin interrupciones y por ultimo disminuye el porcentaje de paquetes desechados por los enrutadores:

confiabilidad. MPLS impone un marco de trabajo orientado a conexión en un ambiente de Internet basado en IP (Internet Protocol) y facilita el uso de contratos de tráfico QoS exigentes. (Lloyd, 2001, p.87)

1.5.4 Requerimientos de las clases de servicio CoS

La ITU-T define 6 clases de servicio, en las que resume los requerimientos de los diferentes tráficos así como el rendimiento que el cliente debería percibir en los extremos de la red del ISP. Cabe mencionar que estos parámetros se han pensado para conexiones del tipo T1 1.544Mbps y/o E1 2.048Mbps. Las clases así como los requerimientos de las diferentes clases de servicio que se explicarán se basan en mediciones en los extremos de las redes de los usuarios que han contratado el servicio, esto quiere decir que se puede atravesar la red así como los nodos de un solo ISP como también se puede atravesar las redes así como los nodos de más de un ISP. El proceso de envío y el tratamiento que será aplicado al tráfico de las aplicaciones a través de la red debe ser transparente al usuario que ha solicitado el servicio.

Clase 0: Aplicaciones en tiempo real de alta Interacción. Estas aplicaciones se caracterizan por ser altamente sensibles no solo al retardo sino a la variación de este, el jitter. Poseen una alta interacción entre ambos puntos extremos de la red. El retardo promedio IPTD que se requiere como máximo es 100ms, la variación del retardo debe estar por debajo de 50ms, se requiere una tasa de pérdida IPLR menor a 3 10− y que la tasa de errores IPER no supere 4 10−. En este grupo de aplicaciones encontramos Voz sobre IP VoIP, Video Teleconferencia VTC.

Clase 1: Aplicaciones en tiempo real Estas aplicaciones se caracterizan por ser sensibles no sólo al retardo sino a la variación de este, es decir, el jitter pero no requieren parámetros tan rígidos como la Clase 0 descrita anteriormente. El retardo promedio IPTD que se requiere como máximo es de 400ms, la variación del retardo debe estar por debajo de 50ms, se requiere que la tasa de pérdida IPLR sea menor a 3 10− y que la tasa de errores IPER no supere 4 10−. En este grupo de aplicaciones encontramos Voz sobre IP VoIP, Video Teleconferencia VTC pero, dependiendo de la localización de los puntos extremos, con una interacción menor y una calidad cualitativa menor percibida en los extremos.

Clase 2: Transacciones de datos con alta interacción Estas aplicaciones se caracterizan por ser la alta interacción a pesar de no ser multimedia y/o de tiempo real. El retardo promedio IPTD que se requiere en el límite como máximo es de 100ms, la variación del retardo no se especifica dado que tiene prioridad de descarte, pero se requiere que la tasa de pérdida sea menor a 3 10− IPLR y que la tasa de errores IPER no supere 4 10−. En este grupo de aplicaciones encontramos tráfico de señalización.

Clase 3: Transacciones de datos Estas aplicaciones se caracterizan por ser la interacción a pesar de no ser multimedia y/o de tiempo real pero con menores requerimientos que la clase anterior. El retardo promedio IPTD que se requiere en el límite como máximo es de 400ms, la variación del retardo no se especifica dado que tiene prioridad de descarte, pero se requiere que la tasa de pérdida sea menor a 3 10− IPLR y que la tasa de errores IPER no supere 4 10−. En este grupo de aplicaciones encontramos tráfico de señalización menos rígido respecto a los parámetros.

Clase 4: Exclusivo para aplicaciones de bajas pérdidas. Estas aplicaciones se caracterizan por tener como principal requerimiento una baja pérdida de paquetes correspondientes al tráfico marcado. El retardo promedio IPTD que se requiere como máximo es de 1000ms, la variación del retardo no se especifica dado que tiene prioridad de descarte frente a otros tráficos de mayores requerimientos, pero se requiere que la tasa de pérdida IPLR sea menor a 3 10− y que la tasa de errores IPER no supere 4 10−. En este grupo de aplicaciones encontramos tráfico de señalización y/o de transacción de corta duración, flujo de video o videostreaming.

Clase 5: Aplicaciones Tradicionales de Redes IP Estas aplicaciones tradicionales de las redes IP sin calidad de servicio, es decir, sus requerimientos no son rígidos en muchos aspectos. El retardo promedio IPTD, la variación del retardo, la tasa de pérdida IPLR y la tasa de errores IPER no se encuentran especificados dado que trabajan bajo el esquema de Best Effort en el cual solo se especifica y se espera que el tráfico llegue a los diferentes destinos. En este grupo de aplicaciones encontramos las aplicaciones tradicionales como correo electrónico email, FTP File Transfer Protocol, HTTP Hyper Text Transfer Protocol, entre otros.

Indicar además que la ITU-T especifica que los requerimientos de los tráficos que no han sido especificados en las recomendaciones, el ISP debe ofrecer una calidad mínima a los usuarios pero no se especifica cual debe ser esta pero recomienda que el Retardo de transferencia de paquetes IP IPTD no se deba exceder los 1000ms.

Las Clases de Calidad de Servicio especificadas anteriormente están sujetas a facilidades técnicas de la red del ISP. La ITU-T en esta recomendación indica que los requerimientos de Retardo de transferencia de paquetes IP IPTD de 100ms no siempre se pueden alcanzar así como otros parámetros de estas mismas clases como de las otras clases explicadas tales como la presencia de paquetes espurios. El ISP debe de especificar los parámetros que se proporcionarán como Calidad de Servicio (QoS) a los diferentes clientes, tratando de acercarse a las expectativas según las facilidades de red que se tenga.

Clase 6: Emulación de circuitos TDM con alta interacción Estas aplicaciones se caracterizan por emular circuitos TDM Time (División Multiplexing) con alta interacción. El retardo promedio IPTD que se requiere como máximo es de 100ms, la variación del retardo es de 50ms, y se requiere que la tasa de pérdida IPLR sea menor a 5 10− y que la tasa de errores IPER no supere 6 10−. En este grupo de aplicaciones entra a tallar un parámetro de Radio de Reordenamiento IPRR (Packet Reordering Ratio), un parámetro que se aplicaría a tráficos TCP o para tráficos semejantes a UDP en el envío de los datagramas pero con un campo destinado para el reordenamiento en el destino. En este grupo de aplicaciones encontramos a la transferencia de televisión de alta calidad por Internet aún bajo estudio, transferencias TCP de alta capacidad y aplicaciones que se basan en emulación de circuitos TDM.

Clase 7: Emulación de circuitos TDM Estas aplicaciones se caracterizan por emular circuitos TDM (Time División Multiplexing). El retardo promedio IPTD que se requiere en el límite como máximo es de 400ms, la variación del retardo es de 50ms, y se requiere que la tasa de pérdida IPLR sea menor a 5 10− y que la tasa de errores IPER no supere 6 10−. En este grupo de aplicaciones también entra a tallar un parámetro de Radio de Reordenamiento IPRR (IP Packet Reordering Ratio), un parámetro que se aplicaría a tráficos TCP o para tráficos semejantes a UDP en el envío pero con un campo destinado para el reordenamiento en el destino. En este grupo de aplicaciones encontramos a la transferencia de televisión por Internet aún bajo estudio, transferencias TCP y aquellas aplicaciones que se basan en emulación de circuitos TDM pero con una interacción y sensibilidad menor a la clase antes explicada. (Lloyd, 2001, pp.88-92)

1.5.5 Tecnologías para el soporte de QoS

En la actualidad, el soporte de Calidad de Servicio está basado principalmente en dos arquitecturas estándar: La arquitectura de Servicios Integrados (IntServ) y la Arquitectura de Servicios Diferenciados (DiffServ). La Arquitectura de Servicios Integrados es utilizada principalmente en

Redes de Acceso debido a que se adapta fácilmente a las necesidades de recursos de los usuarios pero a su vez tiene problemas de escalabilidad debido al agotamiento de los recursos de la red.

Por otro lado, la Arquitectura de Servicios Diferenciados es muy escalable (soporta una gran cantidad de usuarios) pero a cambio, no puede adaptarse fácilmente a las necesidades de recursos de los usuarios. Por tanto, DiffServ es utilizada principalmente en Redes de Transporte. Una tercera parte dentro de este escenario son las redes MPLS (Multi-Protocol Label Switching) que soportan los principios de Ingeniería de tráfico.

Adicionalmente, MPLS puede complementarse con la Arquitectura de Servicios Integrados o con la Arquitectura de Servicios Diferenciados para soportar QoS de una mejor manera en una Internet. Estas tecnologías se explicarán a continuación. (Deering, 2002, p. 77)

1.5.5.1 Intserv y diffserv

Varios mecanismos son los que utiliza MPLS para dar estabilidad de QoS y CoS dentro de su red. En el modelo InterServ (Integrated Services), RSVP obtiene los requerimientos para establecer un flujo de tráfico con QoS, permitiendo a los distintos LSR las negociaciones necesarias para generar un tráfico garantizado y además parámetros o recursos como ancho de banda y latencia end to end.) El modelo DiffServ (Differentiated Services) del IETF.

Define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio (CoS), otorgando un servicio no necesariamente garantizado para el curso del tráfico con diferentes prioridades. Para ello se emplea el campo ToS (Type of Service), en la cabecera de paquete IP para proveer esta clasificación.

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP.

De este modo, una red MPLS puede transportar distintas clases de tráfico, ya que el tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP.

Entre cada par de LSR exteriores se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. Por ejemplo, un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico Best-effort, tres niveles de servicio, primero, preferente y turista, que, lógicamente, tendrán distintos precios. Mientras que InterServ ofrece ancho de banda garantizado para el tráfico, no provee escalabilidad u operabilidad en grandes redes, por otro lado la arquitectura DiffServ, es una alternativa escalable pero no provee de una garantía total.

Recientemente la IETF workgroup se ha enfocado en la combinación de elementos de DiffServ e ingeniería de tráfico, para dar servicios garantizados de flujos de datos MPLS dentro de la red. La información DiffServ en la cabecera IP es mapeada e introducida dentro de la etiqueta de información de los paquetes MPLS.

QoS puede ser y es generalmente implementado en el borde de la red MPLS donde el usuario comienza con la transmisión de los paquetes que requieren un tráfico en tiempo real. (*Srisuresh, 2006, p.47)*

1.5.5.2 Arquitectura de servicios integrados

Arquitectura IntServ En este tipo de arquitectura se usa el campo Flow Label de IPv6 para la identificación de los flujos que se enviarán o se envían a la red IP. En base a este campo se requerirá a la red y a los nodos que la conforman una asignación de recursos correspondiente. Para el funcionamiento de esta arquitectura se hace uso de un protocolo de reserva de recursos RSVP. La petición se hace de origen a destino, en los cuales los routers intermedios entrarán a un estado PATH STATE lo que significa que los routers certifican que tengan los recursos necesarios para la transferencia de datos.

El receptor envía por estos mismos routers un mensaje de confirmación con los que los routers entrarán a un estado RESERVATION STATE con lo cual se confirma que la red está preparada para el envío de información a la red. El estado en el cual el router ha aceptado la transferencia del tráfico correspondiente se llama SOFT STATE. Dentro de esta arquitectura se tienen dos tipos de servicio según los recursos que se necesiten: Guaranteed Rate Service o Controled Load Service según lo que se especifique en el LSA con el ISP. En el primero los recursos se comportan como un Circuito Virtual, es decir, los recursos se encuentran dedicados al cliente; en la segunda, los recursos se

solicitan a la red y si esta los posee se los asigna de manera dinámica, es decir, cada vez que los necesite. (Hesselbach, 2001: 52)

En esta aproximación se hace reserva de recursos por flujos. Un flujo es una cadena de paquetes que fluyen por la red desde una aplicación en un ordenador origen hasta una aplicación en un ordenador destino. La reserva de recursos debe establecerse previamente en cada uno de los Encaminadores que hacen parte del camino entre los dos terminales. Para ello cuando una aplicación desea iniciar una comunicación debe seguir los siguientes pasos: a. La fuente inicia el establecimiento de una reserva describiendo primero a la red las características del flujo y b. La red puede aceptar este nuevo flujo de aplicación sólo si hay suficientes recursos para comprometerse con los recursos solicitados.

Una vez la reserva es establecida, la aplicación puede enviar sus paquetes a lo largo del camino reservado y la red cumplirá su compromiso. IntServ trabaja bajo el supuesto de que la red tiene más recursos de los que se le solicitan. En la práctica esto no se cumple siempre pues en la medida que la red reserva recursos estos no estarán disponibles para otras comunicaciones, por lo que IntServ presenta problemas de agotamiento de recursos. El principal parámetro de Calidad del Servicio con el que se compromete IntServ es el Retardo por Paquete, específicamente el Límite de Retardo del Peor Caso. Los requisitos de los recursos. (Hesselbach, 2001: 52)

El plano de control (Control Plane): Para establecer la reserva de recursos, una aplicación primero caracteriza su flujo de tráfico y especifica los requisitos de QoS. A este proceso se le llama en IntServ: Especificación del Flujo (Flow Specification). La solicitud de establecimiento de reserva de recursos es entonces enviada a la red. Cuando un Encaminador recibe la solicitud, realiza dos tareas:

a. Interactúa con el módulo de Encaminamiento para determinar el siguiente salto al que debe ser enviado la solicitud de reserva.

b. Tiene que coordinar con el Control de Admisión para decidir si hay suficientes recursos para comprometerse con los recursos solicitados.

Para realizar el establecimiento de la reserva a lo largo del camino de los paquetes es necesario utilizar un protocolo de establecimiento de reserva de recursos. El protocolo que usa IntServ para este efecto es RSVP (Resource Reservation Protocol). Una vez completado el establecimiento de la reserva, la información del flujo reservado es instalada en la Tabla de Reserva de Recursos. Esta información es

usada para configurar el módulo de Identificación de Flujos (Flow Identification) y el módulo de Planificación de Paquetes (Packet Scheduler) en el Plano de Datos. (Rick Gallaher., 2006, p.74)

El plano de datos (Data Plane): Cuando llegan los paquetes al Encaminador, el módulo de Identificación de Flujos (también llamado Clasificador) selecciona los paquetes que pertenecen a los flujos reservados y los coloca en las colas apropiadas. (*Srisuresh, 2006, p.57)*

1.5.5.3 Arquitectura diffserv

En este tipo de arquitectura se usa el campo DSCP Differentiated Service Code Point el cual se encuentra dentro del campo DS Differentiated Services también llamado Traffic Class. Esta clase de arquitectura es muy usada actualmente ya que es capaz de poder aceptar diferentes requerimientos de las aplicaciones y por asignarles prioridades a los tráficos.

Para el funcionamiento de esta arquitectura no se necesita ningún protocolo de reserva de recursos como RSVP ya que no es necesario efectuar ninguna clase de petición a los nodos que conforman la red. El procesamiento y el trato que se le dará a los tráficos dependerán únicamente de los valores que se tengan en el campo DSCP ya que cada valor tiene un significado distinto con respecto a requerimiento de recursos de red, al no reservar recursos en la red para el envío de los diferentes paquetes, no se tiene una garantía de QoS como se tenía en IntServ por lo que el tráfico de baja prioridad puede verse afectado si la red se sobrecarga con tráfico de alta prioridad.

Para evitar esta situación se le asigna a cada categoría un SLA. El SLA es negociado con el ISP previamente y generalmente posee carácter estático. Los clientes pueden solicitar un determinado caudal en la categoría que necesiten según las necesidades de la red. Los routers de entrada de la red del proveedor son los responsables del control de admisión o Policy Control, así podrán colocar el valor correspondiente en los paquetes salientes para que sean tratados cada según su categoría dentro de la red del ISP.

El problema de la arquitectura DiffServ es el procesamiento que se debe de hacer a los diferentes tipos de tráfico ya que se tienen prioridades diferentes, por ejemplo, que hacer si un paquete de menor prioridad es procesado cuando uno con mayor prioridad llega a la cola del router.

Véase que el manejo de colas conocidas como RED (Random Early Detection), WRED (Weighted Random Early Detection) y DWRED (Distributed WRED) y otras más recientes como PQ (Priority Queuing), CQ (Custom Queuing), WFQ (Weighted Fair Queueing), CBWFQ (Class Based WFQ) requieren de un procesamiento extra de los routers que no siempre se puede conseguir de manera económica.

Actualmente esta arquitectura es usada ya que ofrece escalabilidad, no sobrecarga la red y si bien no ofrece una garantía de QoS se acepta muchas veces lo que se ofrece con esta arquitectura. Cabe resaltar que las políticas deben de ser muy bien especificadas en el SLA con el ISP ya que, como se mencionó antes, esta arquitectura se basa principalmente en el etiquetado o valor del campo DS de IPv6 o ToS de IPv4.(Thomas,2006,p.35)

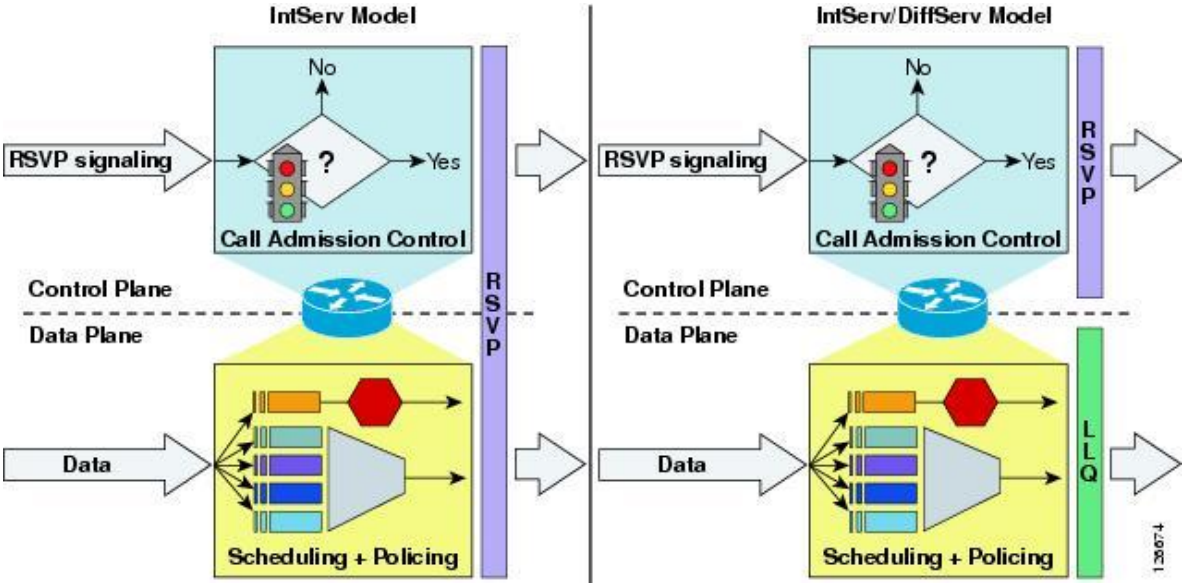


Figura 10- 1: Diagrama Modo de operación IntServ/DiffServ

Fuente:(Cisco, 2011)

1.6 Arquitectura mpls y calidad de servicio QoS en una red ip

La arquitectura MPLS nos provee de un circuito virtual o LSP a través de los diferentes nodos que conforman la red MPLS. Gracias a este tipo de funcionamiento, el circuito virtual creado provee de un trato igualitario a los diferentes tráficos que se envían bajo a un mismo túnel LSP bajo una etiqueta FEC en particular. Estudios relacionados a la Calidad de Servicio en diferentes escenarios

son de interés actualmente dado que, a comparación con las demás arquitecturas, MPLS ofrece escalabilidad, simplicidad, velocidad, entre otros. Las facilidades que ofrece esta arquitectura para la implementación de Calidad de Servicio son las que se explicarán a continuación: (Wischik, 2014: 77)

Velocidad frente al esquema de enrutamiento IP. En efecto, la conmutación de etiquetas es más rápida y eficiente en primer lugar porque se produce en la capa inmediatamente anterior a la capa de red. En segundo lugar, el envío o forwarding se hace en base a un campo específico de la cabecera de la tecnología de conmutación; véase el caso de Frame Relay cuyo campo de identificación de camino es el DLCI Data Link Connection Identifier, en el caso de ATM el campo de identificación es el VCI Virtual Circuit Identifiers. En MPLS, el campo de identificación de camino es el campo Label el cual representa una FEC y un camino en la red. En tercer lugar, el proceso de clasificación del tráfico solo se da en los routers de entrada y el proceso inverso en el router de salida.

Procesamiento más rápido de la cabecera MPLS, En el caso particular de MPLS solo se necesita tener en cuenta los campos Label, TTL para el envío del tráfico y en ciertos casos dependiendo del tipo de SLA que se haga, los campos correspondientes a Stacking para envío interdominio y el campo Experimental EXP para implementar prioridades. En el caso de IP, se deben de procesar muchos campos como dirección origen, destino, TTL (IPv4), opciones (IPv4), Hop Limit (IPv6), Payload, entre otros campos lo cual retrasa el envío y procesamiento de los paquetes en los nodos de la red, además de que este proceso se repite en cada nodo de la red. (Wischik, 2014: 77)

Facilidad de Implementación. Cualquiera de las formas que existe para el correcto funcionamiento de la arquitectura MPLS requiere de poca señalización entre los nodos. Las contramedidas que se pueden tomar en caso de fallas, protocolos de enrutamiento, entre otras tecnologías de capas superiores y/o inferiores no afecta el funcionamiento de la arquitectura, es decir, para cualquier cambio en cualquier capa la arquitectura se amolda a los posibles cambios sin la intervención del administrador de la red MPLS. (Wischik, 2014: 77)

Adaptabilidad frente a la Capa de Red como a la Capa de Enlace la arquitectura MPLS se localiza entre la capa de red y la capa de enlace, se vale de la conmutación para el envío del tráfico y de los protocolos de enrutamiento para la creación de las tablas de conmutación y de rutas alternas para diferentes fines. Como se puede observar, MPLS utiliza la capa superior inmediata así como la inferior pero su funcionamiento no depende de estas. Además, MPLS se adapta perfectamente a las

tecnologías de capa de enlace; tales como ATM, PPP, Frame Relay, la Familia Ethernet; así como a cualquier tecnología de capa de red como IPv4, IPv6. (Wischik, 2014: 77)

El cambio se da en el Software y no en el Hardware. Los nodos que conformarían la red MPLS necesitan solo los procesos correspondientes al manejo de MPLS independientemente de las tecnologías y funcionamiento de la capa de enlace y la capa de red. Para equipos actuales basta con una actualización al sistema operativo de los routers que conforman la Backbone.

Se acomoda a los modelos de Calidad de Servicio (QoS) de la ITU-T. Gracias al campo experimental EXP el cual cuenta con 3 bits, se puede priorizar los diferentes tipos de tráficos cursados en el mismo túnel LSP. Nótese que con 3 bits podemos obtener 8 tipos de prioridades, lo cual coincide con el número de clases que ha sido propuesta por la ITU-T. Esta característica se suma al hecho de que MPLS es capaz de reservar recursos a través de un mismo así como de diferentes dominios.
Puede entenderse que una Clase de Servicio pueda ser implementada bajo una reserva de recursos para ciertos tipos de tráficos provenientes de un cliente y dentro de esta reserva de recursos se daría prioridad a los tráficos que la necesiten. (Wischik, 2014: 77)

Permite la implementación de Ingeniería de Tráfico. Gracias a nuevos protocolos de enrutamiento como a mejoras a otros protocolos de capas superiores, MPLS tiene la capacidad de cambiar dinámicamente de ruta. Las nuevas rutas pueden ser generadas por protocolos de capa de red destinados a crear la tabla de enrutamiento bajo ciertas métricas, así también se aplicarán ciertas políticas en estos mismos protocolos para una mejor evaluación de los recursos de la red.

Además estudios sobre posibles alternativas, impacto en la Calidad de Servicio (QoS) se llevan a cabo actualmente como la utilización del protocolo RSVP-TE RSVP.

Reserva de Recursos Intradominio MPLS. Gracias al túnel LSP que se crea para el envío de los tráficos correspondientes, se asegura que la red pueda soportar los requerimientos solicitados dado que si fuese el caso contrario, el túnel no puede establecerse. (Wischik, 2014: 77)

Así mismo, con el uso de algoritmos de enrutamiento como de protocolos de reserva de recursos RSVP, se puede asegurar una correcta asignación de recursos a los tráficos correspondientes según dirección de destino, origen, puertos, entre otros. A diferencia de la arquitectura IntServ, el protocolo RSVP utilizado en la reserva de recursos de MPLS no requiere el procesamiento y la asignación de

recursos que se necesitaba en IntServ por lo que lo convierte en muy adecuado para los fines antes mencionados. (Wischik, 2014: 77)

Garantía de Calidad de servicio sobre el esquema IP. A diferencia del esquema actual de Internet Best Effort y de DiffServ, los cuales poseen un comportamiento salto por salto o hop by hop, es decir, no dan una garantía total sobre el envío del tráfico que se inserta a la red IP. MPLS, por su parte, antes del envío construye un túnel LSP, donde el comportamiento es igual en todos los nodos que constituyen este túnel LSP, es decir, los recursos que se destinan para este tráfico FEC serán destinados para este tráfico exclusivamente hasta que el tráfico acabe y se liberen los recursos asignados y sean tomados por otro requerimiento. (Deering, 2002, pp54-56)

Aunque IntServ tiene un comportamiento muy parecido en lo que respecta a asignación de recursos, MPLS lo hace de red a red, es decir, crea un túnel LSP desde el router origen al router destino pero no de hots a host como lo hace IntServ; otra diferencia entre estas arquitecturas es el hecho que IntServ crea un comportamiento de recursos dedicados por cada flujo en la red, MPLS crea el mismo comportamiento de recursos dedicados pero con la gran diferencia que los mismos recursos pueden ser usados por diferentes tráficos según los requerimientos especificados en el LSA. (Deering, 2002, pp54-56)

Reserva de Recursos Interdominio MPLS. Así como MPLS está habilitado para el envío como también para la reserva de recursos en las redes MPLS en una misma red de un solo proveedor; gracias al campo Stacking de MPLS se puede extender el túnel creado dentro de una sola red a las redes MPLS que se necesitarán atravesar hasta llegar al destino.

En cada dominio MPLS externo se coloca una cabecera adicional al flujo de tráfico, por lo que, el tráfico que poseía una etiqueta será nuevamente etiquetado cuantas veces sea necesario; y estos paquetes se comportarán como paquetes convencionales en esta arquitectura, es decir, al egreso de cada red se les removerá la etiqueta que se les asignó inicialmente. La cabecera MPLS original, es decir, con la que salió de la red MPLS de nuestro proveedor tendrá marcado el campo Stacking en 1. Gracias a esta facilidad de MPLS, la reserva de recursos se extiende cuanto sea necesario de una forma muy sencilla en comparación a otra tecnología. (Deering, 2002, pp54-56)

1.6.1 Codecs

La palabra códec proviene de abreviar las palabras codificación y decodificación. Su función principal es la de adaptar la información digital de la voz para obtener algún beneficio. Este beneficio en muchos casos es la compresión de la voz de tal manera que podamos utilizar menos ancho de banda del necesario.

Algunos codecs, soportados por Asterisk y comúnmente usados en comunicaciones de VoIP, son:

Codecs de Audio:

- G.711
- G729
- GSM (GLOBAL SYSTEM FOR MOBILE COMUNICATIONS).
- ILBC (INTERNET LOW BITRATE CODEC).

Codecs de Video:

- H263
- H263P
- H264

1.6.1.1 G.711

Es uno de los codecs más usados de todos los tiempos y proviene de un estándar ITU-T (Sector de Normalización de las Telecomunicaciones). Viene en dos versiones llamados u-law y a-law. La primera versión se utiliza en los Estados Unidos y la segunda se utiliza en Europa. G.711 es un estándar para representar señales de audio con frecuencias de la voz humana, mediante muestras comprimidas de una señal de audio digital con una tasa de muestreo de 8000 muestras por segundo. El codificador G.711 proporcionará un flujo de datos de 64 kbit/s. El soporte para este códec ya viene habilitado en Elastix. (Landivar, 2011, pp50-57)

1.6.1.2 G.729

También se trata de una recomendación ITU cuyas implementaciones ha sido históricamente licenciadas, o sea que hay que pagar por ellas. La ventaja en la utilización de G.729 radica principalmente en su alta compresión y por ende bajo consumo de ancho de banda lo que lo hace atractivo para comunicaciones por Internet.

Pese a su alta compresión no deteriora la calidad de voz significativamente y por esta razón ha sido ampliamente usado a través de los años por muchos fabricantes de productos de VoIP. G.729 utiliza 8kbit/s por cada canal. Si comparamos este valor con el de G.711 notaremos que consume 8 veces menos ancho de banda, lo cual a simple vista es un ahorro de recursos significativo. Existen variaciones de G.729 que utilizan 6.4kbit/s y 11.8kbit/s.

También es muy común G.729a el cual es compatible con G.729 pero requiere de menos cómputo. Esta menor complejidad se refleja en la calidad de la conversación ya que ésta empeora considerablemente. (Landivar, 2011, pp50-57)

1.6.1.3 GSM.

El estándar que define la tecnología celular GSM (Global System for Mobile communications) incluye este códec. La ventaja de este códec también es su compresión. Acerca de la calidad de voz. GSM comprime aproximadamente a 13kbit/s y ya viene habilitado en Elastix. (Landivar, 2011, pp50-57)

1.6.1.4 ILBC.

Es un códec de VOIP creado originalmente por el sonido global del IP pero hizo disponible (su código de fuente incluyendo) debajo de un restricto pero libera y licencia bastante liberal, incluyendo el permiso de modificarse. El iLBC (Códec bajo de Bitrate del Internet) es un códec LIBRE del discurso conveniente para el IP excesivo robusto de la comunicación de voz.

El códec se diseña para el discurso y los resultados de banda estrecha en un índice binario de la carga útil de 13.33 kbit/s con una longitud de codificación del marco de 30 ms y 15.20 kbps con una longitud de codificación del ms 20. El códec del iLBC permite la degradación agraciada de la calidad del discurso en el caso de marcos perdidos, que ocurre con respecto a los paquetes perdidos o retrasados del IP. (Landivar, 2011, pp50-57)

1.6.1.5 H.263

H.263 es un estándar de la Unión Internacional de Telecomunicaciones (ITU) para la codificación de vídeos. H.263 describe un códec, que en primera línea se concibió para videoconferencias. Está

optimizado para una tasa de bits baja de 64 kbit/s, es decir, velocidad ISDN (Red Digital de servicios Integrados) y un movimiento relativo reducido.

Si bien, el propio estándar no define una tasa de bits concreta. H.263 es un códec de vídeo necesario en las especificaciones técnicas del European Telecommunications Standards Institute o 3GPP para subsistema multimedia IP (IMS), Sistema de mensajería multimedia (MMS) y Transparent end-to-end Packet-Switched Streaming Service (PSS).En las especificaciones 3GPP, vídeo H.263 se utiliza generalmente en el formato contenedor 3GP. (Landivar, 2011, pp50-57)

1.6.1.6 H.263p

También conocido como H.263 más h263p o H.263v2 es básicamente una mejora de H.263 soportada por el Eyebeam de Xten proporcionando una mejora de la calidad de vídeo. Fue diseñado reteniendo completamente el contenido técnico de la primera versión (H.263) del estándar, pero mejorando las capacidades de H.263 añadiendo varios anexos que pueden mejorar substancialmente la eficiencia de la codificación y proporcionar otras capacidades (tales como una robustez mejorada frente la pérdida de datos en el canal de transmisión). (Landivar, 2011, pp50-57)

1.6.1.7 H.264

Es un estándar para compresión de vídeo también conocido como MPEG-4, o MPEG-4
AVC (para Advanced Video Coding).La finalidad del proyecto H.264/AVC era crear un estándar capaz de proporcionar Buena calidad de vídeo a Bitrate sustancialmente inferiores que los estándares previos (por ejemplo menos de la mitad del Bitrate de MPEG-2, H.263, o MPEG-4), sin incrementar demasiado la complejidad del diseño para que no fuera impracticable o excesivamente caro de implementar.

Un objetivo adicional era proporcionar suficiente flexibilidad para permitir aplicar el estándar en una amplia variedad de aplicaciones y una amplia variedad de redes y sistemas, incluyendo bajos y altos Bitrate, vídeo de alta y baja resolución, multidifusión, almacenamiento en DVD, redes de paquetes RTP/IP y sistemas de telefonía multimedia ITU-T.(Landivar,2011,pp50-57)

1.7 Elastix

Elastix es un software libre para crear un servidor de comunicaciones unificadas el cual provee juntos un Conmutador IP, eMail, Faxeo y funcionalidad de colaboración. Cuenta con una interface web y tiene funcionalidades como la del módulo Call Center con marcación predictiva. La funcionalidad de elastix está basada en varios proyectos de software libre los cuales son: Asterisk, HylaFAX, Openfire y Postfix, los cuales ofrecen los servicios de conmutador, fax, mensajería instantánea y correo electrónico respectivamente. (Oliva, 2011, p.54)

1.7.2 Ventajas

Elastix provee todo lo que se necesita para implementar comunicación unificada en este proyecto. La interfaz web de administración basada en FreePBX hace que la configuración y administración de Asterisk sea muy sencilla. Al utilizar software libre de comprobada calidad y estabilidad elastix es muy estable una vez que se ha configurado correctamente. Así también es muy sencillo una vez funcionando agregar nuevos módulos y actualizar la interface a una nueva versión. (Oliva, 2011, p.54)

1.7.3 Desventajas

Las desventajas de elastix son más que nada basadas en la experiencia de la persona que lo implementa, es decir, para una persona puede resultar un poco confusa la interfaz de administración, y para un experto en Asterisk puede resultar demasiado pesada ya que hace un uso extensivo de macros. Un profesional de T.I.C. experto en Debían GNU/Linux puede encontrar aburrido buscar la ubicación de los archivos de configuración ya que elastix está basada en CentOS, y cosas por el estilo. Por lo tanto dependiendo de la experiencia de la persona que vaya a implementar una solución basada en Asterisk con elastix serán las desventajas y desventajas. (Oliva, 2011, p.54)

CAPITULO II

MARCO METODOLOGICO

2.1 Introducción

En el capítulo se observa el esquema del diseño de red emulado y probado para su posterior implementación a los equipos reales, la configuración y convergencia del sistema, la selección, instalación, configuración y prueba de las herramientas necesarias para el tráfico de los datos y la integración de todos los elementos para el posterior análisis, tomando en cuenta que un ISP normal cuenta con una red de CORE con equipos de mayor Gama, para este trabajo las pruebas a realizarse fueron con fines académicos se limitó a usar equipos de la academia CISCO, sin embargo el sistema debe posibilitar el análisis de calidad de servicio para un entorno de CORE mpls.

Entre las herramientas está el servidor elastix, con el cual se crea la central pbx, los softphone para realizar las llamadas entre usuarios, el software Ostinato para inyectar un tráfico externo a la red, wireshark para el análisis y captura de datos en la red convergente.

La red mpls se implementó con 4 routers cisco 2900 con un iOS que soportara la configuración de los protocolos requeridos, 4 switch 2960, un router AP que permita conectar los equipos móviles al sistema de red mpls.

2.2 Diseño de la arquitectura de red MPLS

Para empezar se diseñó la red en un emulador para las pruebas de configuración y conectividad, así asegurar la convergencia de la infraestructura de red

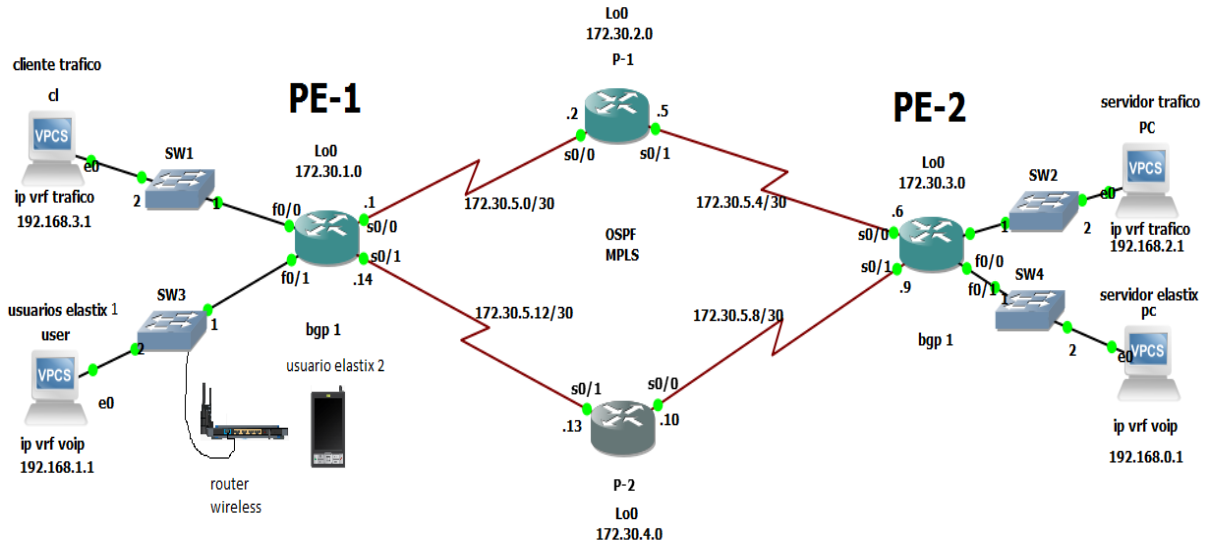


Figura 1- 1: Arquitectura de pruebas MPLS

Realizado por: Crow. W 2016

2.3 Desarrollo de la arquitectura de red emulada

Como etapa de investigación para el desarrollo de la red se usó el emulador GNS3 en el cual se realizó las configuraciones necesarias para comprobar conectividad y convergencia del sistema, posteriormente implementar en los equipos reales. Cabe recalcar que al contar con una red de CORE mpls facilita el crecimiento escalable de la misma.

2.4 Direccionamiento

En la fig. 2.2 se muestra la conexión de los equipos a través de sus interfaces visualizando su direccionamiento. En la tabla 1-2 se visualiza las direcciones de enrutamiento de cada router.

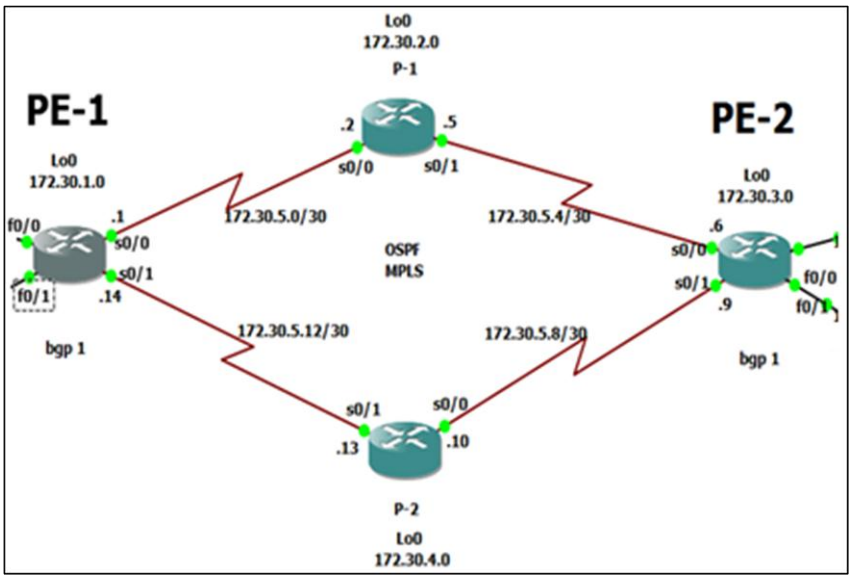


Figura 2- 1 Direccionamiento

Realizado por: Crow. W 2016

Tabla 1-2 Direccionamiento

Tabla de direccionamiento					
Routers	F0/0	F0/1	Lo0	S0/0	S0/1
PE-1	192.168.3.1/24	192.168.1.1/24	172.30.1.1/32	172.30.5.1/30	172.30.5.14/30
P1			172.30.2.1/24	172.30.5.2/30	172.30.5.5/30
PE-2	192.168.2.1/24	192.168.0.1/24	172.30.3.1/32	172.30.5.6/30	172.30.5.9/30
P2			172.30.4.1/24	172.30.5.10/30	172.30.5.13/30

Realizado por:(Walther Crow)

2.5 Configuración de los equipos en GNS3

Con el diseño de la red y direccionamiento establecido se determinó la configuración necesaria de cada equipo para lograr establecer una arquitectura acorde a las prestaciones requeridas para el previo análisis y pruebas.

2.5.1 Verificación de la red OSPF

Luego de direccionar la red se procedió a configurar el protocolo ospf para establecer las adyacencias e intercambiar información de la topología. Se procede a verificar las redes conectadas y conocidas por cada router.

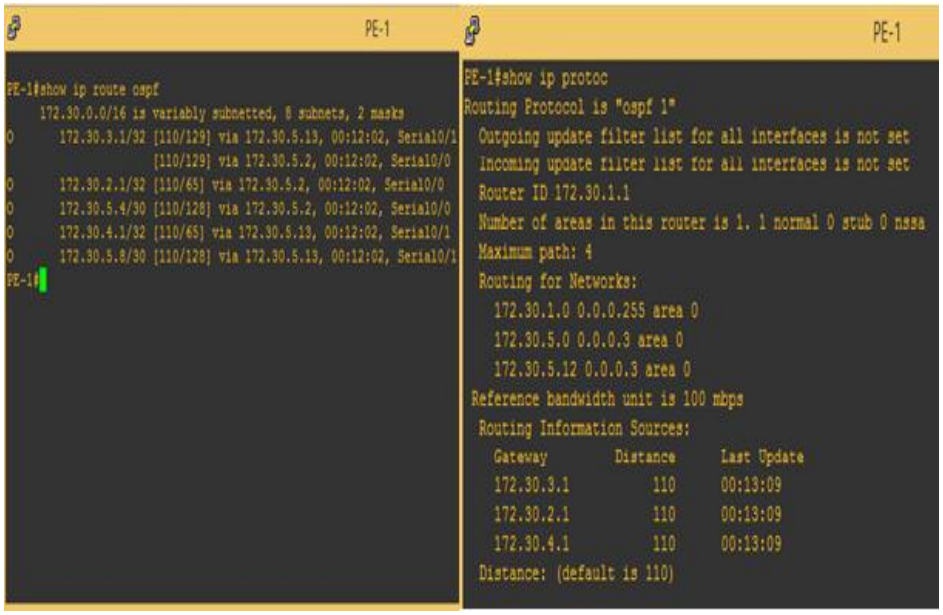


Figura 3- 2 Verificación de OSPF

Realizado por:(Walther Crow)

Se puede observar el protocolo OSPF configurado en el router PE-1, sus redes conectadas directamente y los router vecinos, se configura OSPF en los routers P1, PE-2, P2 de igual manera anunciando sus interfaces conectadas directamente.

2.5.2 Constatar red MPLS

Luego de configurar el protocolo OSPF necesario para que MPLS funcione ya que necesita de conectividad se procede a verificar en la fig. 4-2 que este protocolo este esté activado correctamente.

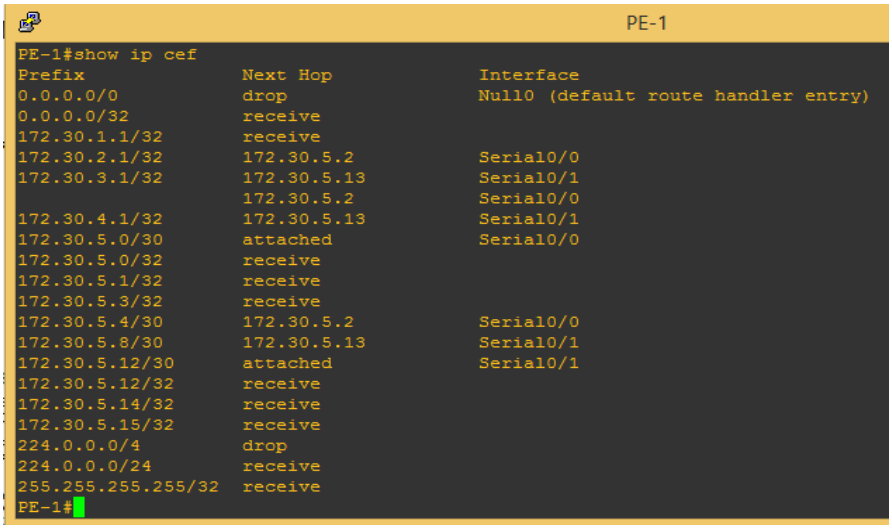


Figura 4- 2 Configuración de OSPF

Realizado por: Crow. W 2016

En la fig. 5-2 Se observa la tabla de forwarding y se verifica que el cisco express forwarding (cef) este activo, necesario para habilitar MPLS.

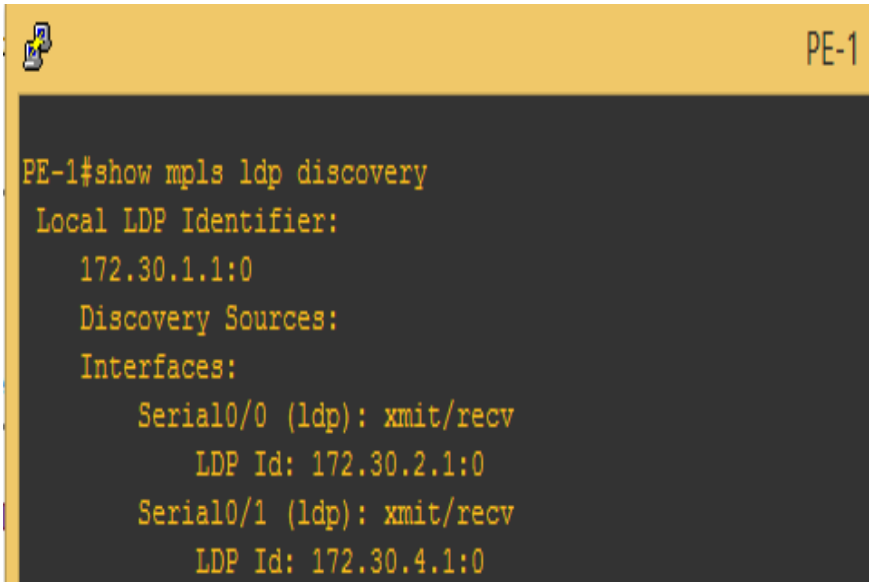


Figura 5- 2 Figura de forwarding

Realizado por: Crow. W 2016

Se visualiza en la fig. 6-2 que conoce el LDP local y sus vecinos para establecer las adyacencias.

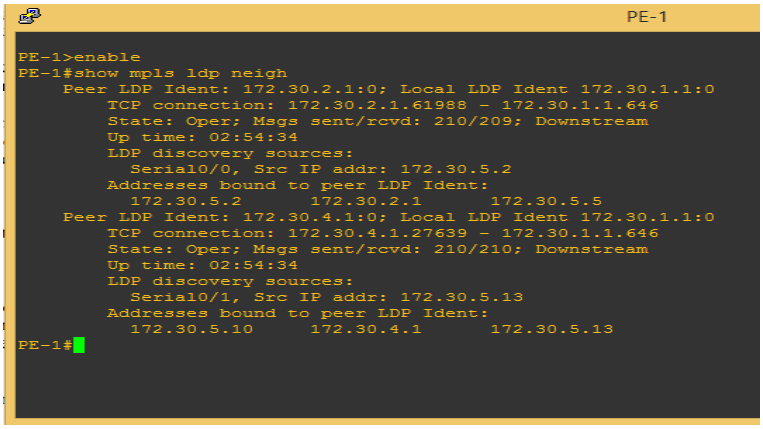


Figura 6- 2 Conocimiento de LDP

Realizado por: Crow. W 2016

Se muestra las adyacencias LDP y la condición en la que se encuentra conectado a los vecinos, MPLS se configura en cada interfaz de los routers P1, PE-2, P2 de la misma manera que en el router PE-1.

2.5.3 Verificar configuración de BGP

Luego de haber configurado MPLS para el transporte se necesita configurar MP-BGP así crear las sesiones de extremo a extremo entre el servidor y los clientes, por el hecho que MPLS solo creo el túnel de transporte pero se necesita aislar el trafico dentro del túnel, por tal hecho se procedió a crear las sesiones BGP entre el router PE-1 (clientes) y el router PE-2 (servidor) para crear el enlace entre estos dos equipos, haciendo uso de un protocolo de la familia de BGP como es el MP-BGP (multi Protocol BGP) declarando el protocolo VPNV4 que es una vrf el cual me aísla el tráfico entre vrf.

2.5.3.1 Configuración del router PE-1

Verificamos la configuración de BGP del router PE-1 declarando el VPNV4 protocolo encargado de permitir crear la vrf todo esto dentro de la familia BGP, ubicando la dirección de enlace que se quiere alcanzar, además se observa en la fig. 7-2 el sistema autónomo al que pertenece (BPG 1)

PE-1

```
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 172.30.3.1 remote-as 1
 neighbor 172.30.3.1 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 172.30.3.1 activate
  neighbor 172.30.3.1 send-community extended
 exit-address-family
```

Figura 7- 2 Configuración del router PE-1

Realizado por: Crow. W 2016

2.5.3.2 Configuración del router PE-2

Se evidencia la configuración del router PE-2 de igual sistema autónomo del router que se quiere alcanzar a través del enlace creado entre los dos, la configuración es la misma que el router PE-1 con la diferencia de la dirección IP que se quiere alcanzar como se evidencia en la fig. 8-2

PE-2

```
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 172.30.1.1 remote-as 1
 neighbor 172.30.1.1 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 172.30.1.1 activate
  neighbor 172.30.1.1 send-community extended
 exit-address-family
```

Figura 8- 2 Configuración del Router PE-2

Realizado por: Crow. W 2016

2.5.3.3 Configuración de las vrf

En la fig. 9-2 se evidencia la configuración de las vrf que este caso se ha necesitado de dos una para el tráfico de VoIP de nombre (voip) y la otra para un tráfico externo la cual lleva el nombre de (trafico), Creando el router distinguishers el cual va a cumplir con la función de diferenciar las vrf y denotar a que vrf pertenece. La misma configuración se realiza en el otro extremo del enlace (router PE-2).

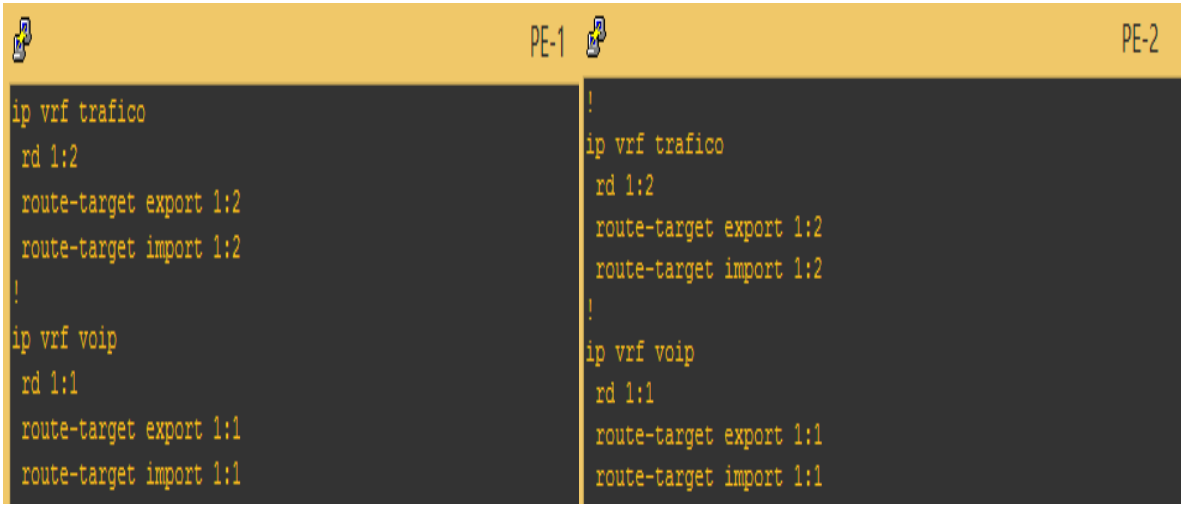


Figura 9- 2 Configuración VRF

Realizado por: Crow. W 2016

Podemos observar en la fig. 10-2 las interfaces configuradas con su respectiva vrf además de su dirección ip en los extremos de los routers PE-1 y PE-2 evidenciando la configuración del forwarding a través del comando ip vrf forwarding y el nombre de la vrf.

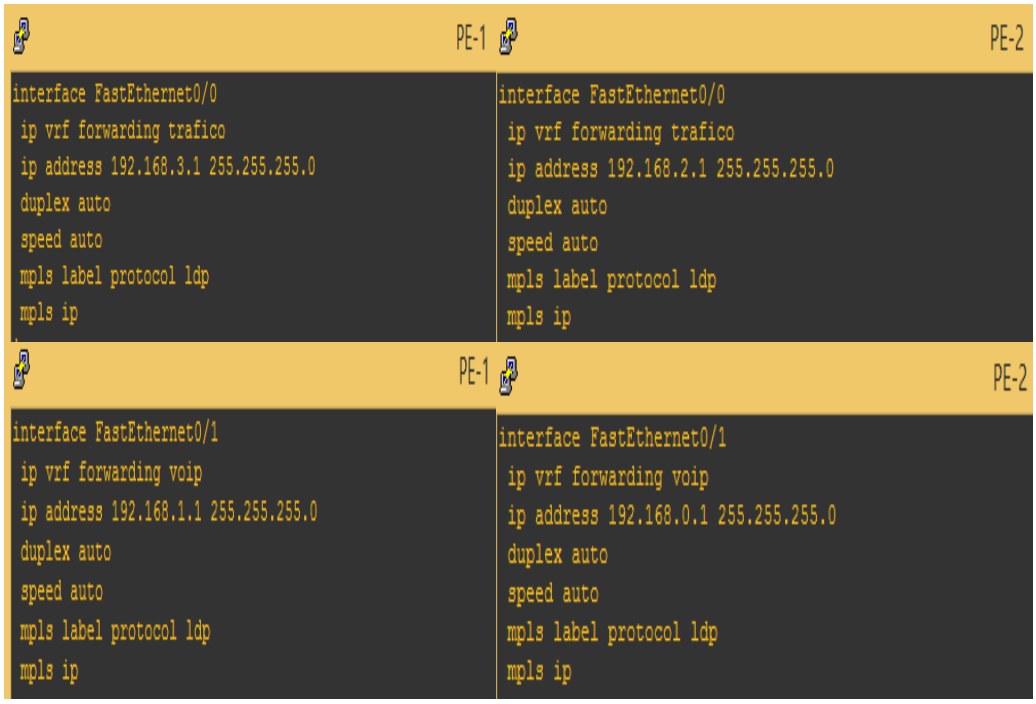


Figura 10- 2 interfaces de VRF

Realizado por: Crow.W 2016

Por último se debe redistribuir las VRF con el comando Redistribute connected para encaminar los paquetes hacia cada prefijo local a través de la propagación de dichos prefijos como se evidencia en la fig. 11-2

Figura 11- 2 Redistribute connected
Realizado por: Crow.W 2016

2.5.3.4 Verificar VRF

Se verifica las VRF, su tabla de enrutamiento la cual es transparente para el usuario con el comando show ip route VRF y el nombre de las VRF creadas (voip, trafico).

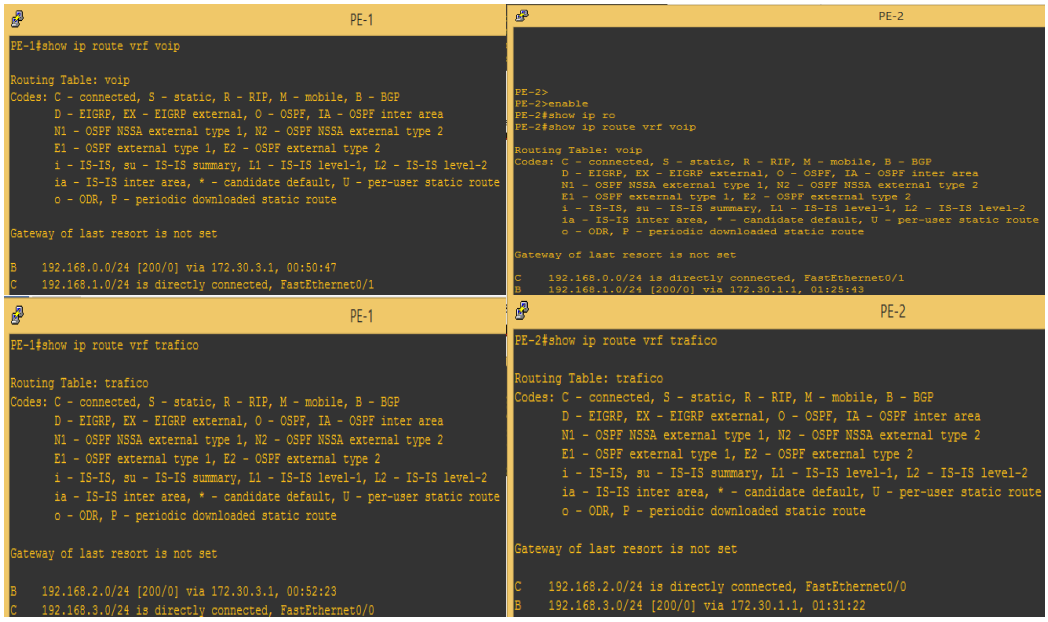


Figura 12- 2 Verificación VRF
Realizado por: Crow.W 2016

Se observa en la fig. 13-2 la IP directamente conectada y la dirección que va alcanzar además de la vía para conectar ambos extremos del cliente y servidor. Por último se realiza un ping entre las VRF del mismo nombre de extremo a extremo así observar si existe comunicación entre cliente y servidor esto verificamos en ambos VRF (voip y tráfico).

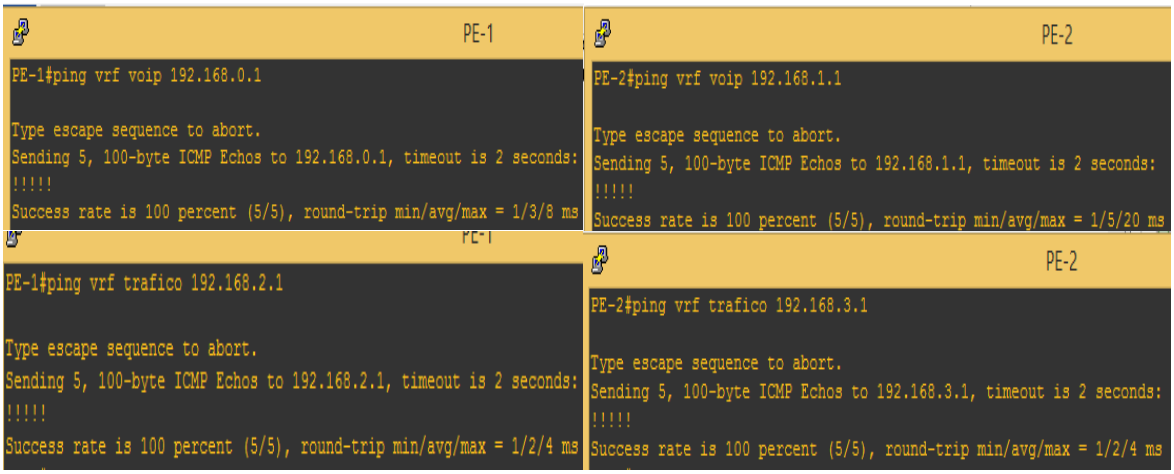


Figura 13- 2 Voip y Tráfico

Realizado por: Crow.W 2016

2.6 Implementación en los equipos físicos

2.6.1 Introducción

En este apartado se observan los equipos físicos que fueron necesarios para montar la infraestructura de red, siendo necesario dispositivos que fueron suministrados por la academia de CISCO ESPOCH e implementados en unos de los laboratorios de CISCO.

Para trabajar con equipos físicos antes se probó la configuración en el emulador gns3, se obtuvo información de los dispositivos cisco (hardware, software) para verificar si admitirían configurar los protocolos necesarios para el montaje de la red, teniendo una visión clara del IOS del equipo y si este software soportaría cada protocolo a configurar.

2.6.2 Descripción de los routers

Para armar y probar la topología de red fue necesario el uso de 4 routers cisco 2900 los cuales cumplían con las especificaciones para la configuración de los servicios a utilizar.

Lo mas importante de estos equipos era conocer si soportarian la configuracion de los protocolo y servicios para el posterior analisis ya con la red convergente.

Los router cisco 2900 cuentan con un IOS software 15M & T. Release 15.0 con soporte para voz, video, calidad de servicio, conmutacion por etiquetas multiprotocolo (MPLS), redes privadas virtuales. Ademas de los protocolos OSPF, BGP, MP-BGP. En la fig. 14-2 se tiene una vision frontal posterior de el router cisco 2900.

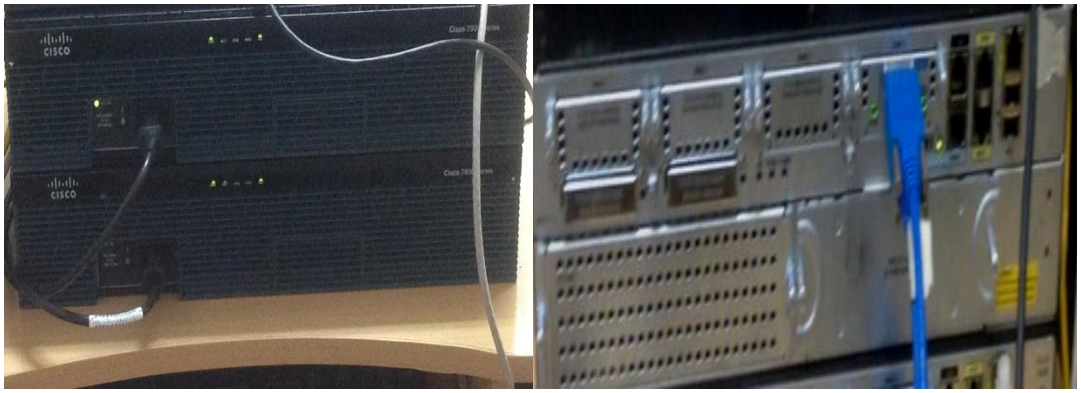


Figura 14- 2 Router 2900

Realizado por: Crow.W 2016

2.6.3 Función de los routers

En este apartado se describe la ubicación y función de cada router ya que antes fue emulado en gns3 para posterior ser configurados en los equipos físicos y se detalla a través de la fig. 15-2 los nombres de cada router.

Figura 15- 2: Routers

Realizado por: Crow.W 2016

Siendo los routers PE-1 (cliente) y PE-2 (servidor) los extremos de la topología de red, los cuales llevan la misma configuración emulada y probada tanto en el emulador como en los equipos físicos.

2.7 Materiales para la conexión de los routers

Se necesitó de los siguientes materiales para la conexión de su etapa de energía, conexión serial, conexión LAN:

Tabla 2-2 Materiales

Cantidad	material
4	Cable serial
4	Cable de poder
4	Cable directo UTP
1	Cable de consola

Realizado por: Crow.W 2016

2.8 Conexión serial

En la fig. 16-2 se muestra la conexión de los cables seriales para intercomunicar a los routers y la conexión de sus salidas giga Ethernet a los usuarios y servidor tanto del Elastix como del inyector de tráfico externo.

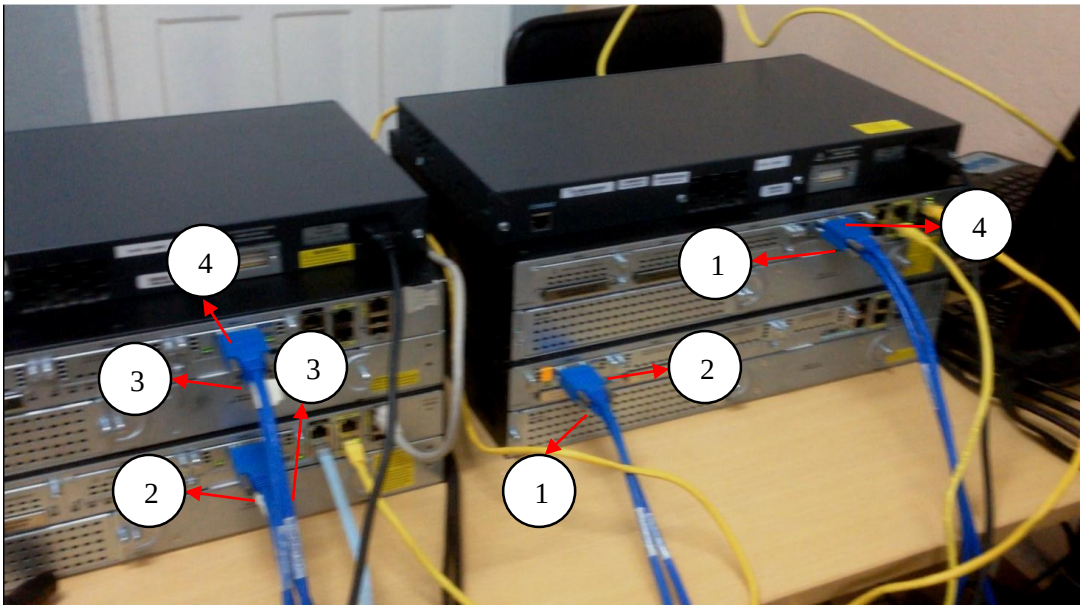


Figura 16- 2 Conexión de cables seriales

Realizado por: Crow.W 2016

En la tabla 3-2 se procede a describir cómo están distribuida las conexiones entre interfaces:

Tabla 3-2 Distribuciones de las conexiones

Numero	descripción
1-1	Corresponde la conexión entre la interfaz serial 0/0/0 del router PE-1 a la interfaz 0/0/0 del router P1
2-2	Conexión entre la interfaz serial 0/0/1 del router P1 a la interfaz serial 0/0/0 del router PE-2
3-3	Conexión entre interfaz serial 0/0/1 del router PE-2 a la interfaz serial 0/0/0 del router P2
4-4	Conexión entre la interfaz serial 0/0/1 del router P2 a la interfaz serial 0/0/1 del router PE-1

Realizado por: Crow.W 2016

2.8.1 Conexión de las interfaces giga Ethernet

En la fig. 17-2 se describe la función de cada interfaz giga Ethernet además de observar su ubicación en el router

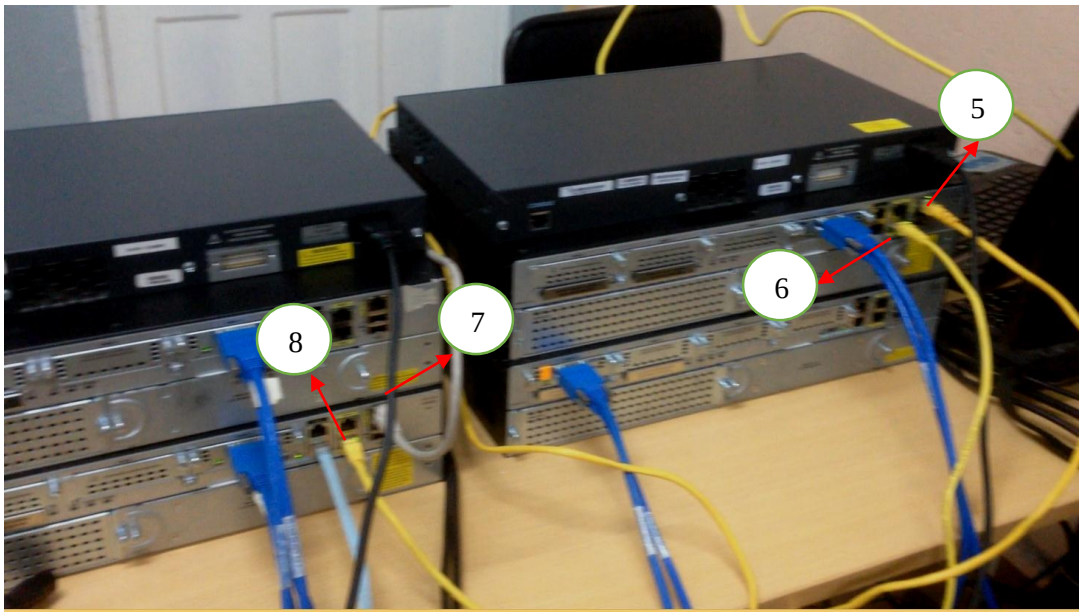


Figura 17- 2 Interfaces Giga Ethernet

Realizado por: Crow.W 2016

Tabla 4-2 Descripción de las interfaces

numero	descripción
5	Corresponde a la interfaz giga Ethernet 0/0 del router PE-1 con la dirección de Gateway de la VRF tráfico del servidor
6	Interfaz giga Ethernet 0/1 del router PE-1 con la dirección de Gateway de la VRF voip cliente
7	Interfaz giga Ethernet 0/0 del router PE-2 con la dirección de Gateway de la vrf trafico cliente
8	Interfaz giga Ethernet 0/1 del router PE-2 con la dirección de Gateway de la vrf voip servidor

Realizado por: Crow.W 2016

2.9 Descripción de los switch

Una vez que se ha conectado y configurado los routers cisco se ha hecho uso de 4 switch 2960 para conectarlos los host. En la fig. 18- 2 se observa la función con la que cumple cada switch.

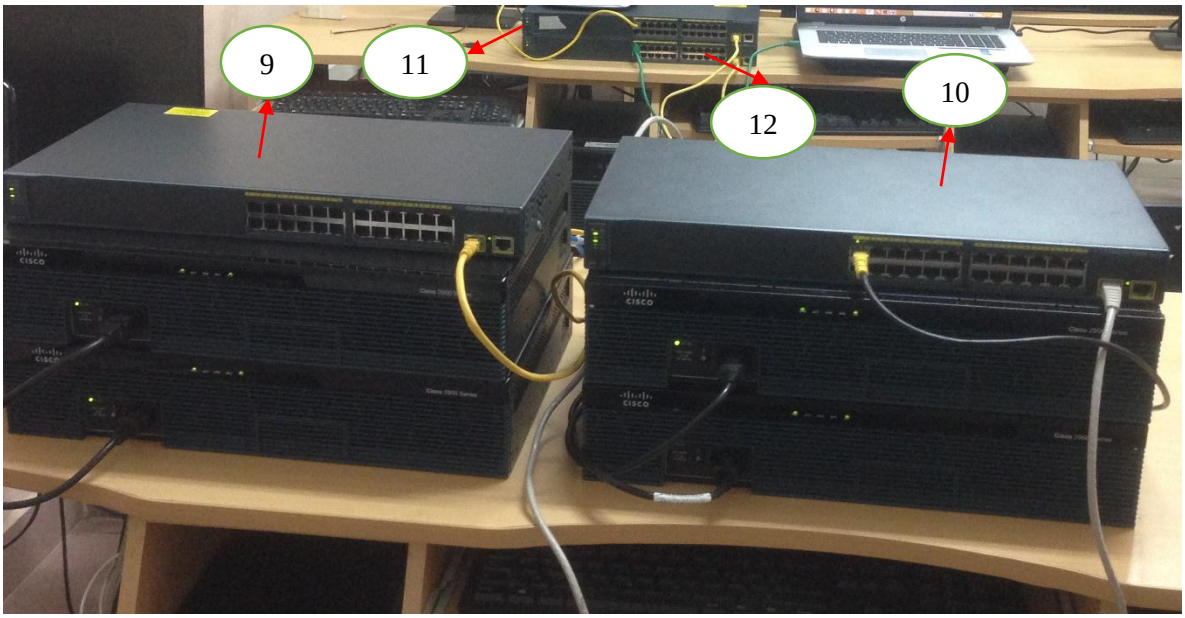


Figura 18- 2 Switch

Realizado por: Crow.W 2016

Tabla 5-2 Descripción de los Switch

numero	descripción
9	Switch-host servidor Gateway vrf trafico
10	Switch-host cliente Gateway vrf trafico
11	Switch-host cliente Gateway vrf voip
12	Switch-host servidor Gateway vrf voip

Realizado por: Crow.W 2016

2.10 Equipos adicionales

Además de los equipos ya descritos anteriormente se hizo uso de 4 computadoras, un router Ap, y un dispositivo móvil los cuales se necesitaron para montar el servidor elastix, servidor de trafico externo, cliente elastix y receptor del tráfico externo, el dispositivo móvil que cumplía con la función de un cliente conectándose a través de router Ap.

2.10.1 Software y herramientas

Corresponde al final de la arquitectura de red luego de haber armado, configurado, y hecho las pruebas de conectividad el último paso fue la utilización del software virtual box, el IOS Elastix, la herramienta de inyección de tráfico OSTINATO y por último el WIRESHARK.

2.10.2 Virtualbox

En esta etapa se hizo uso del virtualizador para instalar el sistema operativo elastix, ya que Virtualbox es un software gratuito y de fácil implementación que prestaba los servicios necesarios para soportar elastix (Centos), además de la asequible comunicación con las tarjetas de red con las tarjetas de red de la PC anfitrión. En la fig. 19-2 se observa el software Virtualbox con la imagen montada elastixtesis.

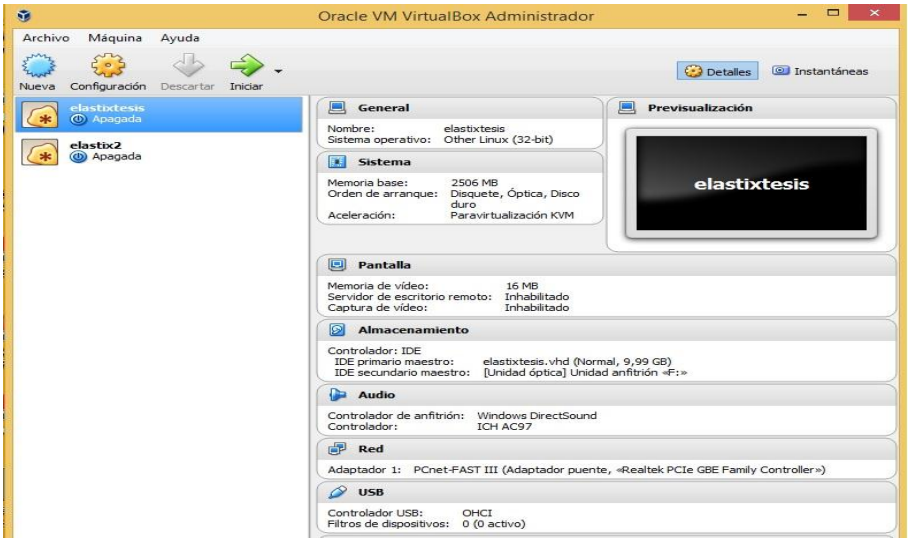


Figura 19- 2 Virtualbox

Realizado por: Crow.W 2016

2.11 Elastix

Como se mencionó el servidor a ser utilizado fue elastix cual instalado en la máquina virtual permitirá crear y controlar e intercomunicar a los usuarios para las llamadas (voip, video llamada).

Elastix es una distribución libre de Centos servidor para intercomunicaciones unificadas el cual se compone en una sola trama de voip, fax, pbx, correo electrónico etc. Su función principal es de incorporar una solución para todas las alternativas de comunicación corporativas.

Se procedió a instalar primero elastix versión 2.5.0 sobre una máquina virtual versión 5.1.6 realizando la instalación con la misma dirección de Gateway de la vrf voip servidor para configurar durante la instalación una ip dentro del rango de la red para acceder a la interfaz web que brinda elastix como entorno amigable para la creación de los usuarios voip. En la fig. 20-2 se observa la interfaz de Centos donde se observa la dirección de la interfaz web 192.168.0.150

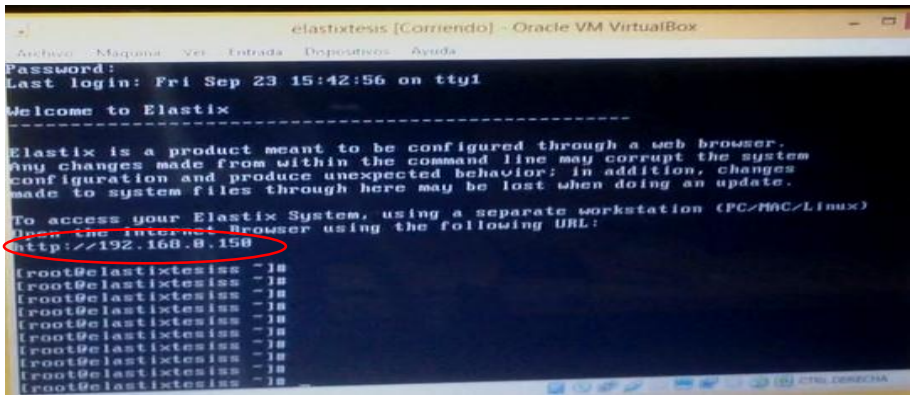


Figura 20- 2 Elastix versión 2.5.0

Realizado por: Crow.W 2016

En la fig. 21-2 se observa la interfaz de Centos con la dirección de ingreso a la interfaz web 192.168.0.150 la cual nos mostrara un entorno más amigable para la creación de los usuarios y la activación de los servicios que se van a utilizar.

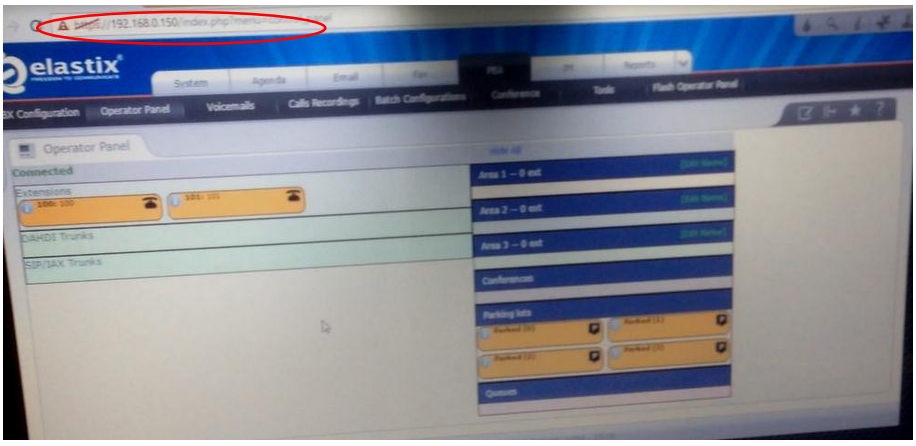


Figura 21- 2 Interfaz web 192.168.0.150

Realizado por: Crow.W 2016

CAPITULO III

3. MARCO DE RESULTADOS

3.1 Introducción

En este capítulo se mostraran las pruebas realizadas a la topología de red MPLS implementada en los laboratorios de CISCO de la Escuela Superior Politécnica de Chimborazo, empezando por la convergencia de la arquitectura comprobando la comunicación entre los host conectados a las respectivas vrf.

Después de tener comunicación entre los host, se procedió a realizar la configuración del servidor elastix, la creación de los usuarios o extensiones y la activación de los servicios para voip y video llamada. Además de la instalación, configuración de los softphone y del inyector de tráfico.

Luego de haber realizado los pasos anteriores ya con el sistema completamente funcional se ejecutó las pruebas respectivas, a medida que se realizó las pruebas se examinó el comportamiento de la red implementado con los equipos físicos en transmisión y recepción. Al verificar la correcta convergencia de las etapas de transmisión y recepción se realizó las pruebas en calidad de servicio y la evaluación de los datos obtenidos.

3.2 Conexión del servidor elastix

Partiendo de lo ya señalado en el anterior capítulo el servidor elastix será montado en una máquina virtual lo cual fue necesario comprobar la correcta comunicación de la máquina virtual con la pc anfitrión y la pc con toda la red.

3.2.1 Creación de los usuarios en elastix

En este apartado se configura los usuarios necesarios para las llamadas, en este caso se ha creado dos usuarios los cuales generaran el trafico voip y video llamada necesarios para el análisis por separado de la calidad de servicio.

Se empezó creando las extensiones en la configuración de la pbx en este caso la primera extensión se le coloco en user 100 la visualización de Display 100.

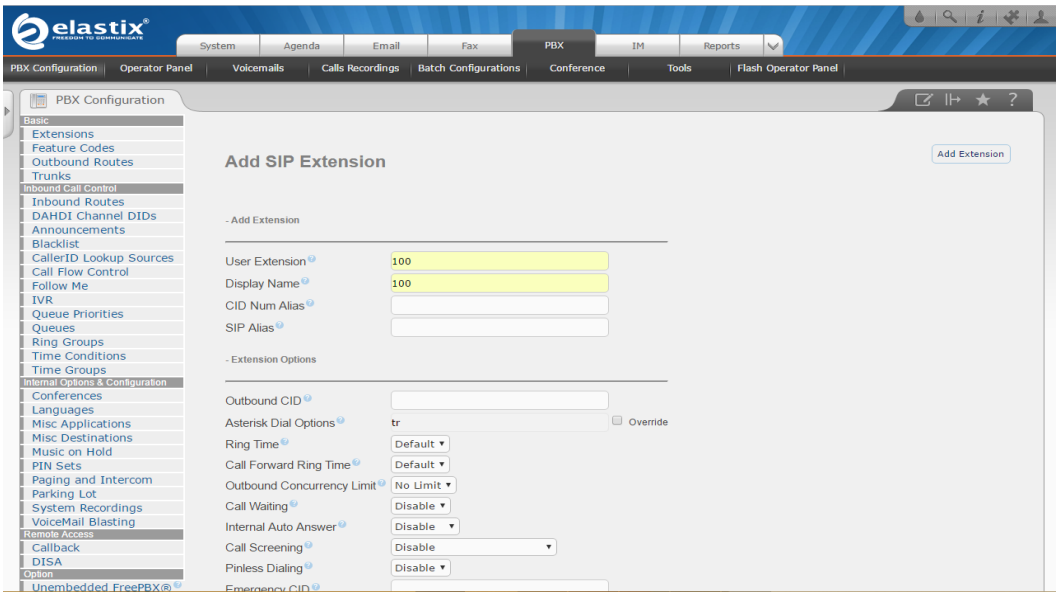


Figura 1- 3 Usuario Elastix

Realizado por: Crow.W 2016

Además durante las pruebas se comprobó que para tener conectividad entre los usuarios era necesario omitir el campo de encriptación SIP.

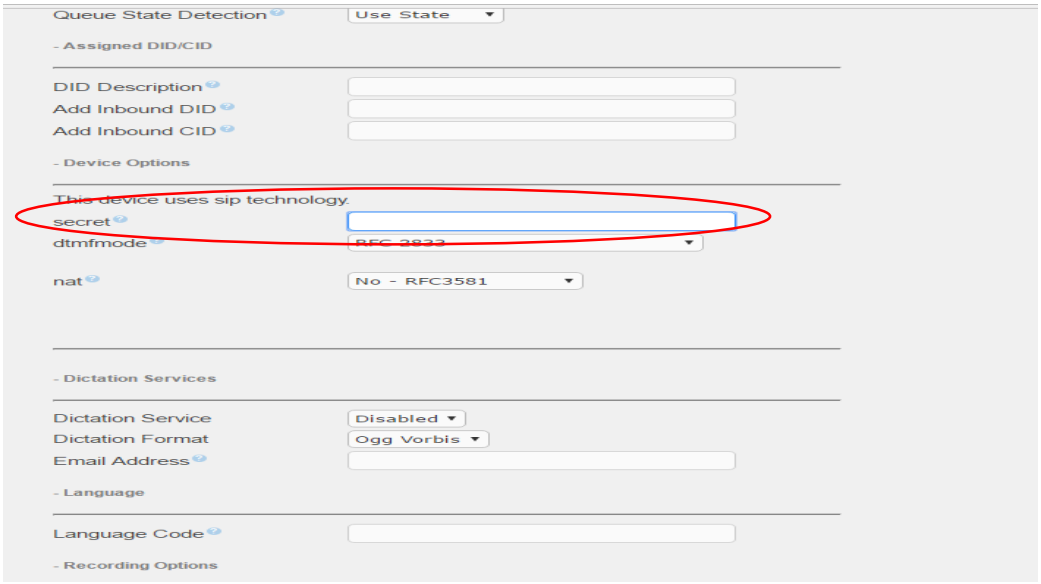


Figura 2- 3: Campo de encriptación

Realizado por: Crow.W 2016

Luego la configuración se la envía para que sea creada muy importante es no olvidar de guardar los cambios para que pueda reconocer el servidor las extensiones.

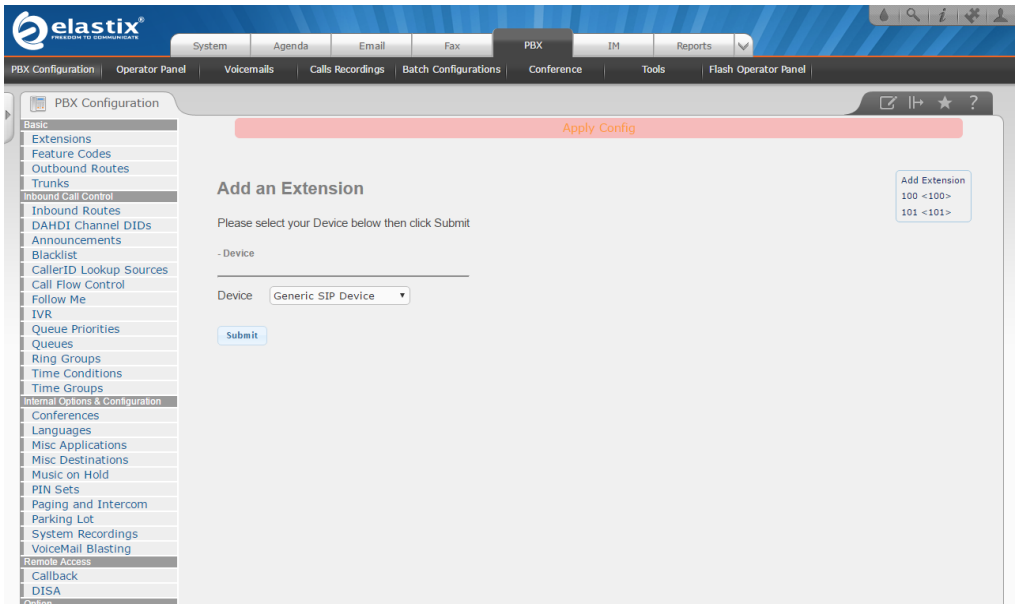


Figura 3- 1 Reconocimiento del elastix

Realizado por: Crow.W 2016

El mismo proceso se debió seguir para crear la extensión 101. El siguiente paso fue crear los usuarios proporcionando un login y nombre el cual se ha ubicado el mismo número de extensión, además del ingreso de una contraseña (1234) y grupo al cual pertenecería en este caso al grupo administración.

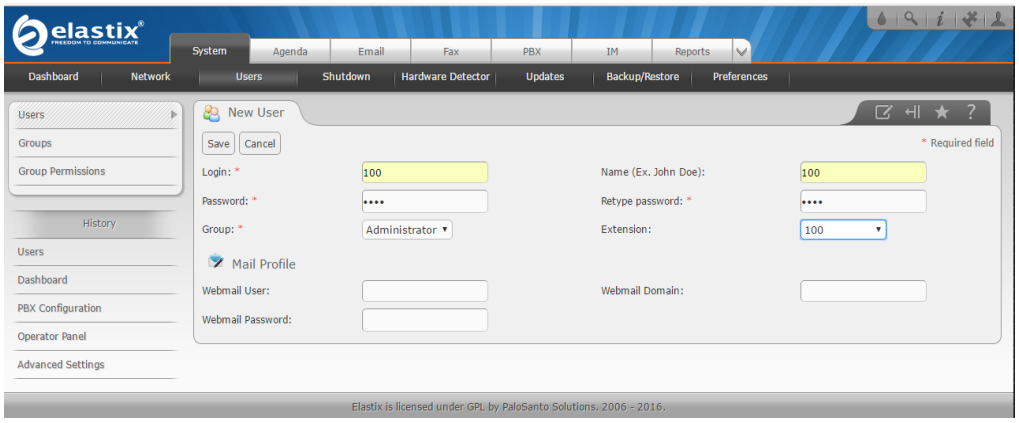


Figura 4- 3 Usuarios

Realizado por: Crow.W 2016

Se guarda para que se creen los usuarios el mismo proceso se realiza para el otro usuario con el cambio de 101 donde se puso 100. En la figura 5-3 se muestra los dos usuarios creados los cuales se usaron para las llamadas.

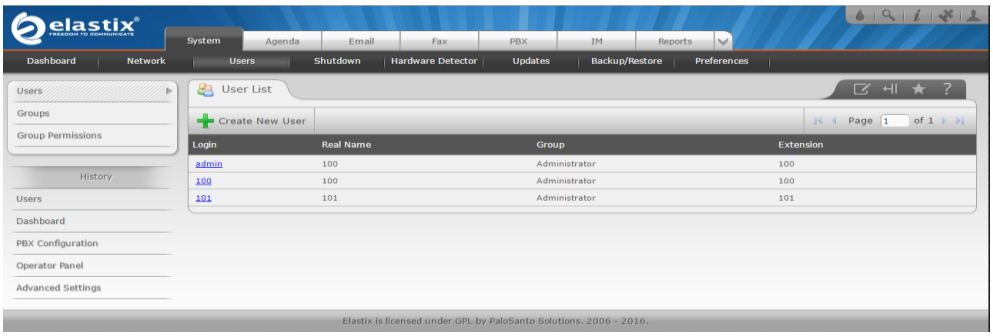


Figura 5- 3 Usuarios utilizados en la llamada

Realizado por: Crow.W 2016

3.2.2 Activar servicio de video llamada

En el aparto anterior una vez configurado los usuarios obtenemos llamadas de audio, pero aún no se puede establecer la comunicación con video el cual es necesario para el análisis propuesto, se procede a la activación del servicio de video llamada el cual elastix nos brinda soporte.

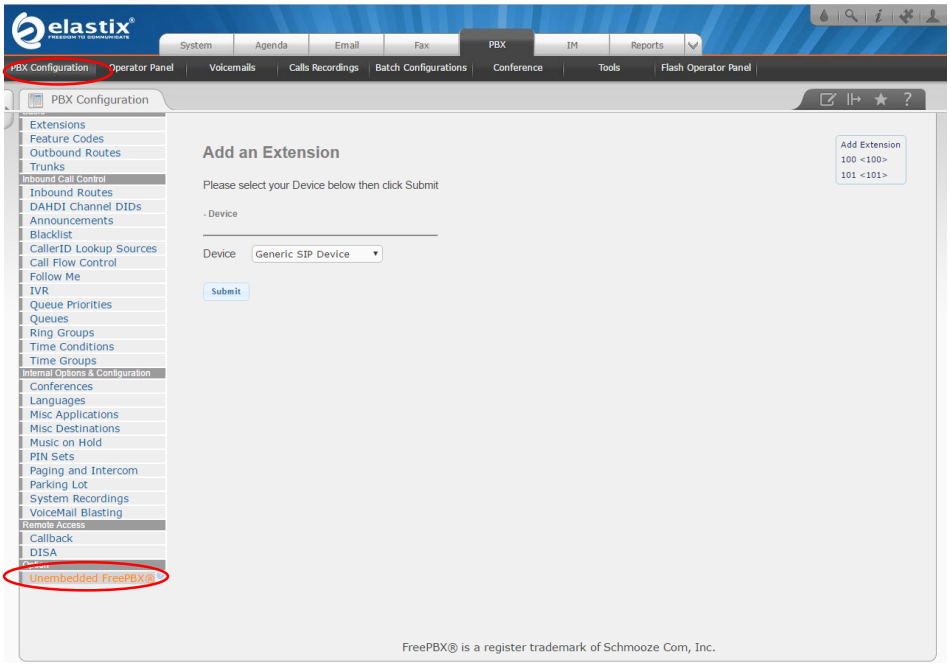


Figura 6- 3 Activación del servicio

Realizado por: Crow.W 2016

Ingresando a la interfaz web que brinda elastix entramos en la configuración pbx y damos clic en el la parte inferior izquierda FREPBX el cual nos destellara una nueva ventana.

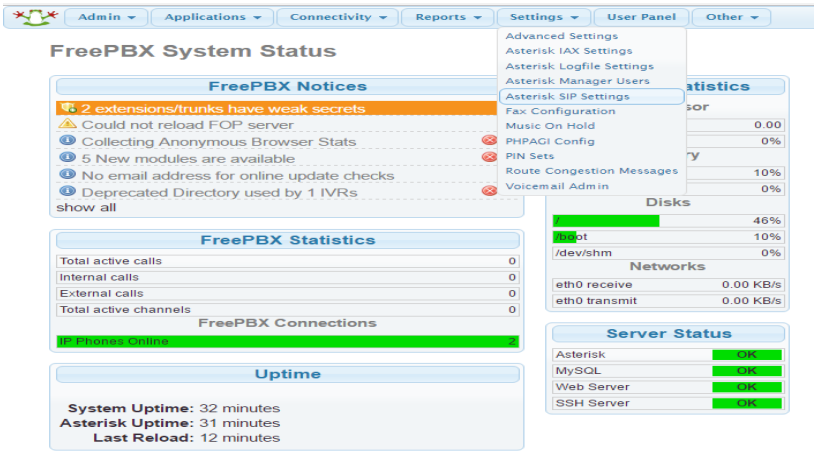


Figura 7- 3 FREPBX

Realizado por: Crow.W 2016

Ingresando a la configuración nos despliega un menú de opciones, se selecciona la configuración SIP de Asterisk. En la Figura 8-3 observamos la ventana que se desplego dando la opción de seleccionar el códec de audio en este caso se ha utilizado el códec G.711 (alaw) además permite activar la opción de video llamada la cual por defecto esta desactivada, una vez activada la opción permite elegir el códec de video el cual se activado el h263plus.

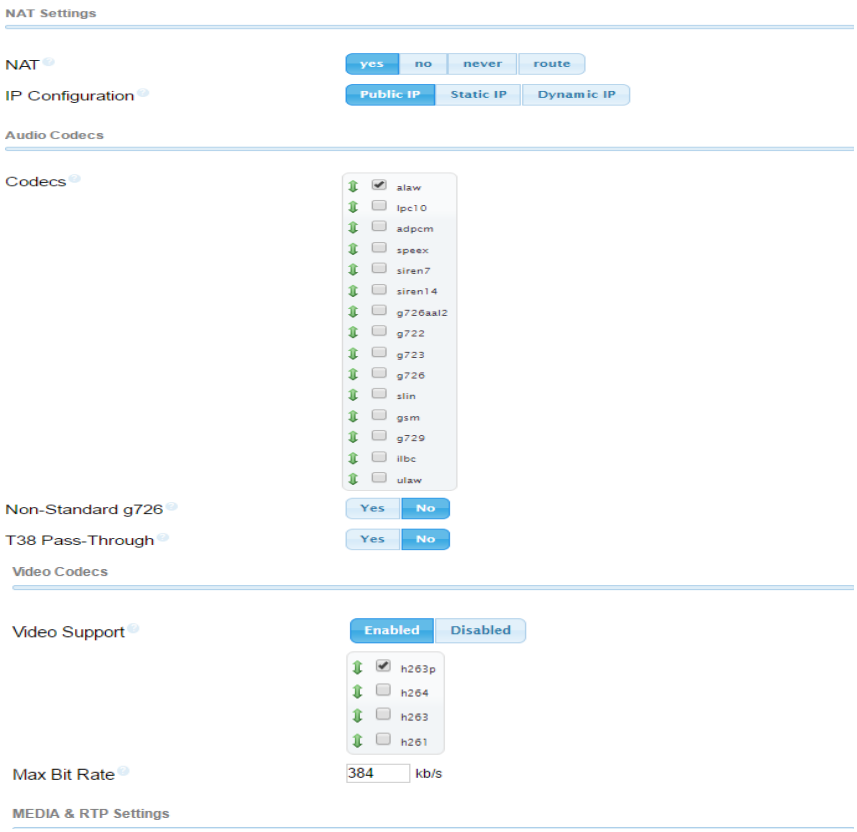


Figura 8- 3 Ventana del Códec de audio y video

Realizado por: Crow.W 2016

3.3 Configuración de Softphone

Para poder realizar las pruebas de comunicación entre usuarios se hizo usó de la aplicación Zoiper instalándolo tanto en el teléfono móvil como la PC. En este apartado se evidencia la configuración de los usuarios en la APP Zoiper y su registro en el servidor elastix.

Figura 9- 3 APP Zoiper

Realizado por: Crow.W 2016

Se crea las cuentas de usuario ingresando los datos que configuramos en el servidor elastix. Nombre de la cuenta (101), la dirección de host del servidor para establecer la comunicación (192.168.0.150) y la clave (1234). El mismo proceso hacemos para la cuenta de Zoiper de la pc cambiando el usuario en este caso se coloca (100). En la fig. 10-3 se observa los que los usuarios han establecido conexión con el servidor.

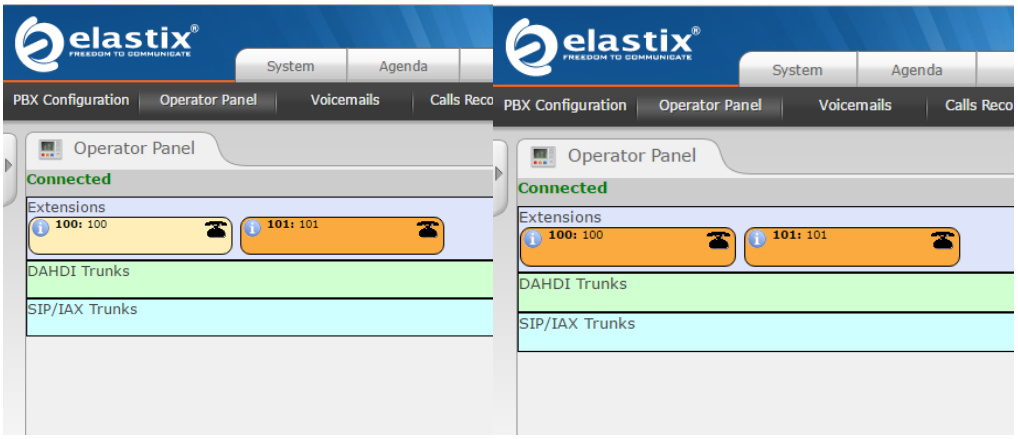


Figura 10- 3 Conexión de los usuarios al servidor

Realizado por: Crow.W 2016

3.4 Pruebas de llamada VOIP

Antes de realizar las llamadas para las pruebas y obtención de los datos para el análisis se consideró dejar habilitado un solo códec de audio y video tanto en el servidor como en los usuarios además de una misma tasa de bits/s.

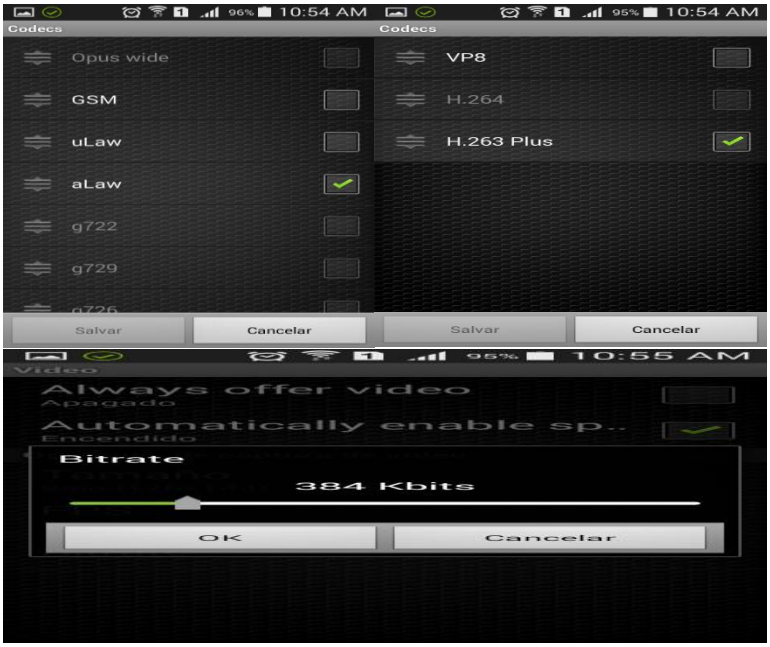


Figura 11- 3 Activación del códec de audio y video

Realizado por: Crow.W 2016

De esta manera el servidor elastix establecería el enrutamiento de las llamadas de extremo a extremo con el mismo códec de audio y video ya que al tener más de un códec activo se detectó el problema ya que el servidor tiene conflictos en la selección del códec y al asignarle diferentes codecs a los usuarios al momento de realizar una llamada se tendría errores en la comunicación. En la figura 12-3 se observa la llamada entrante del usuario 100 al 101.

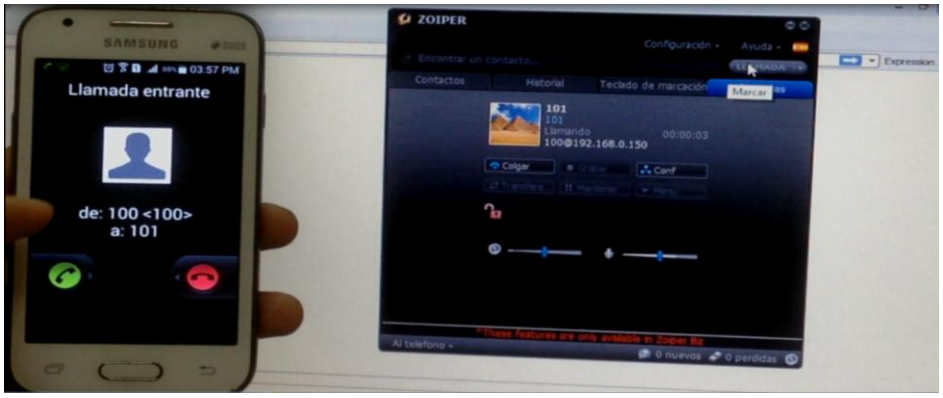


Figura 12- 3 Enrutamiento de llamadas

Realizado por: Crow.W 2016

3.5 Análisis

Para la realización del análisis de los parámetros que determinen la calidad de servicio en una arquitectura de red MPLS se consideró inyectar un tráfico externo, de esta manera el análisis a realizar no sería en condiciones ideales. Se adoptó la necesidad de utilizar un software el cual ingrese a la red MPLS un tráfico externo.

Se hizo uso del software generador de tráfico (Ostinato). El cual permitía inyectar un tráfico externo a la red MPLS mientras se generaba los paquetes con el servidor elastix de esta manera capturar y hacer el análisis de los datos en condiciones reales (de un ISP).

Este es un software (Ostinato) el cual funciona en la modalidad cliente-servidor permitiendo inyectar paquetes por la VRF tráfico hacia la red MPLS. Al inyectar el tráfico por la VRF del mismo nombre se estaría aislando los paquetes de la VRF VOIP y el tráfico externo. Esto con la finalidad de darle un mejor balance de carga y evitar la saturación para no tener riesgo que se descarten los paquetes.

Cabe indicar que se contaba con enlaces seriales con un máximo de ancho de banda de 8Mbps, y para la implementación se trató de simular enlaces de alto desempeño como las que usan las redes CORE reales.

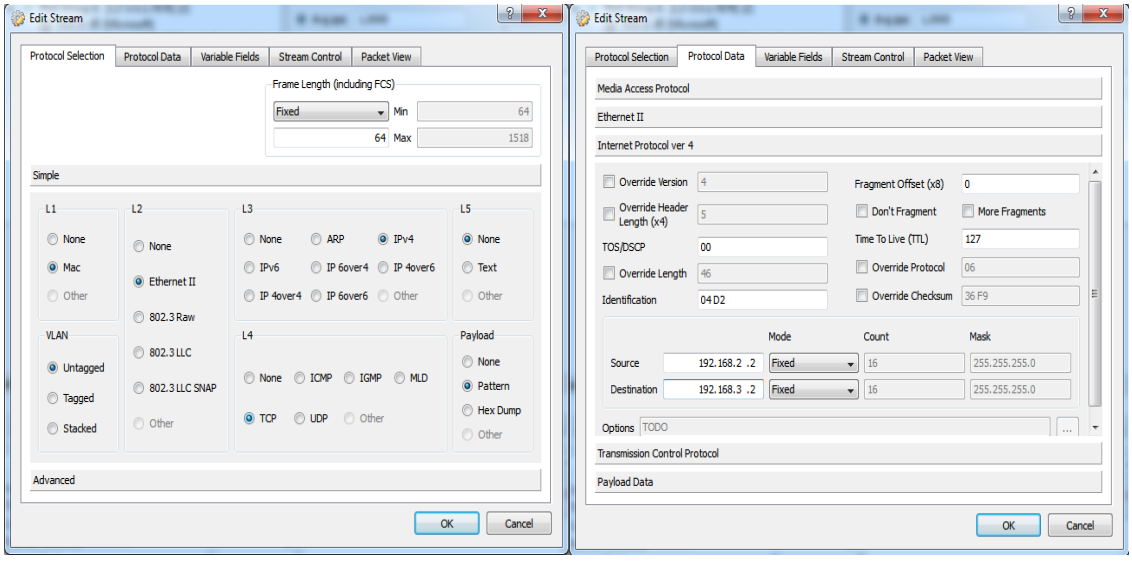
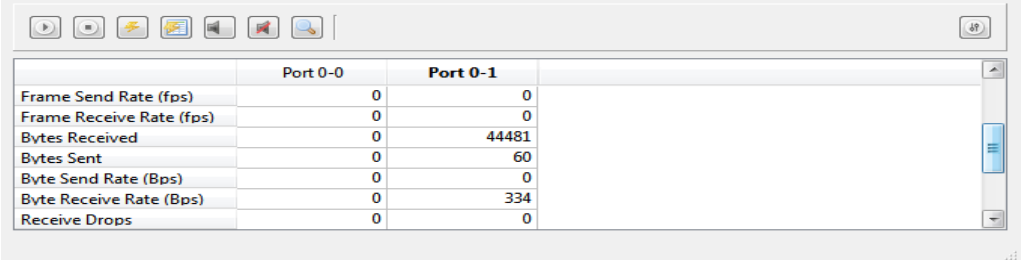


Figura 13- 3 Software Ostinato
Realizado por: Crow.W 2016

En la figura 13-3 se observa el tipo de paquete que ingresara a través de Ostinato además de la dirección de host de la vrf tráfico del servidor (192.168.2.2) hacia la dirección host destino de la vrf tráfico del cliente (192.168.3.2). Después de este proceso se observa en la figura 14-3 el tráfico de los paquetes.



	Port 0-0	Port 0-1
Frame Send Rate (fps)	0	0
Frame Receive Rate (fps)	0	0
Bytes Received	0	44481
Bytes Sent	0	60
Byte Send Rate (Bps)	0	0
Byte Receive Rate (Bps)	0	334
Receive Drops	0	0

Figura 14- 3 Tráfico de paquetes
Realizado por: Crow.W 2016

3.6 Captura de tráfico con WIRESHARK

Una vez realizado lo descrito en los apartados anteriores se procede a capturar el tráfico con el programa wireshark observando primero que el protocolo SIP establezca la peticiones de comunicación entre los usuarios (100-101).

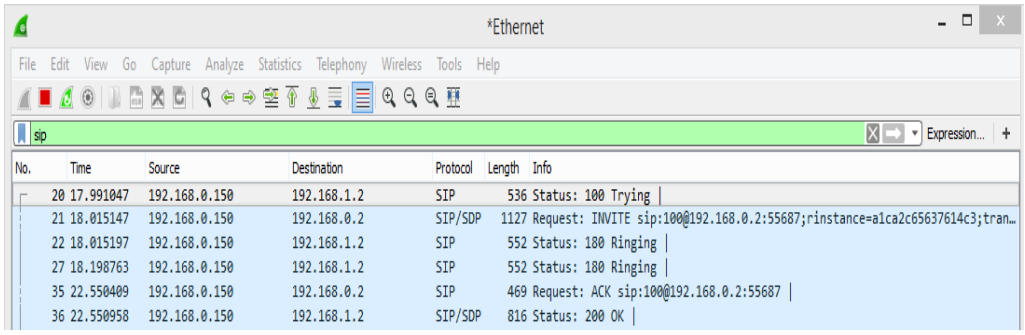


Figura 15- 3 Wireshark

Realizado por: Crow.W 2016

Se visualiza el protocolo SIP al momento de establecer la llamada. Protocolo encargado de la comunicación de sesiones interactivas con elementos multimedia como voz y video. Además en la fig. 16-3 se evidencia al momento de realizar la llamada se visualiza el protocolo RTP necesario para el establecimiento de sesión en tiempo real y el códec que se está usando para la llamada G.711.

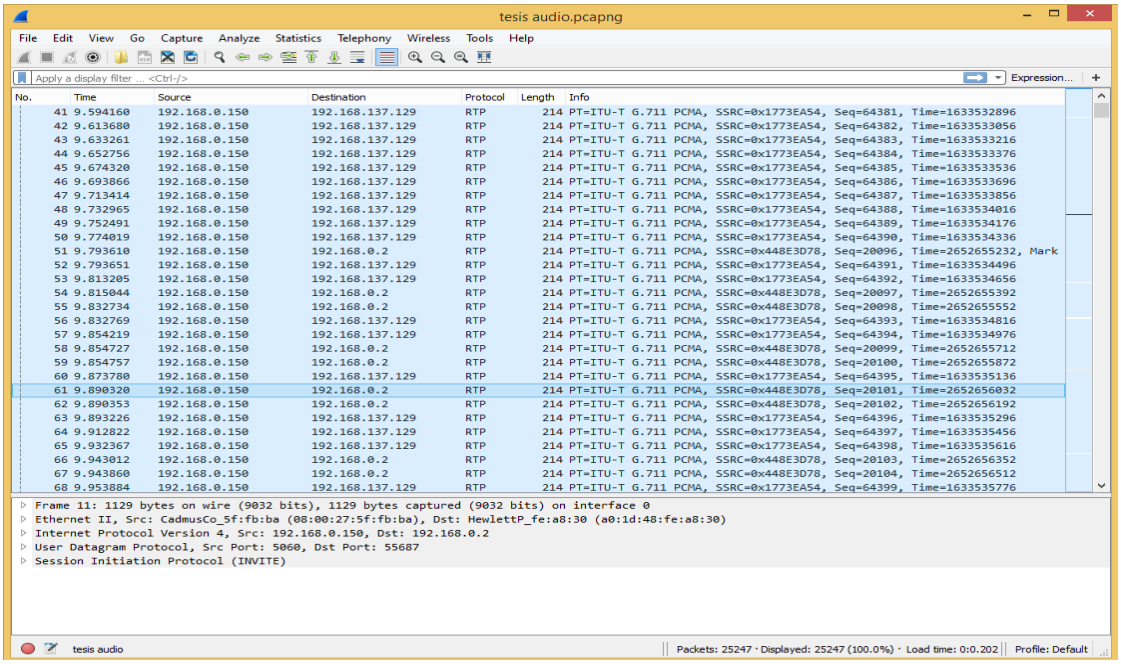


Figura 16- 3 Protocolo SIP

Realizado por: Crow. W 2016

3.7 Prueba de video llamada

El siguiente proceso era analizar la calidad de servicio al establecer una llamada de video realizando los mismos pasos del apartado de voip ingresando un tráfico externo.

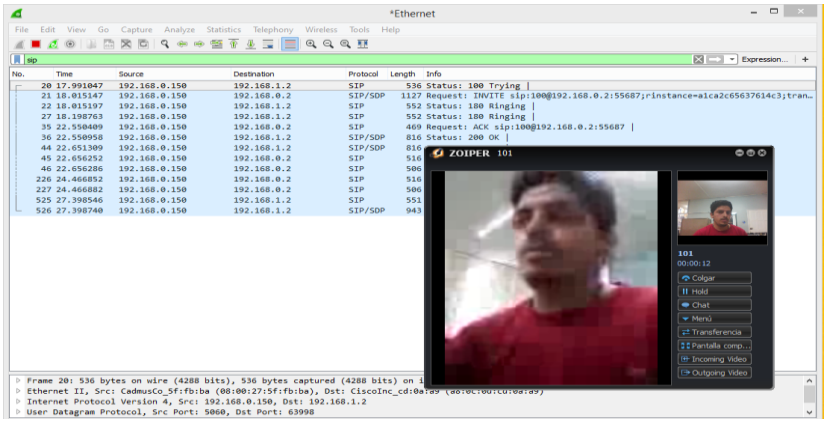


Figura 17- 3 Llamada de video
Realizado por: Crow. W 2016

En la Figura 17-3 se observa el establecimiento de sesión con el protocolo SIP además de visualizar la transferencia de video. Además en la Figura 18-3 observamos el protocolo RTP con el códec de video establecido H.263p.

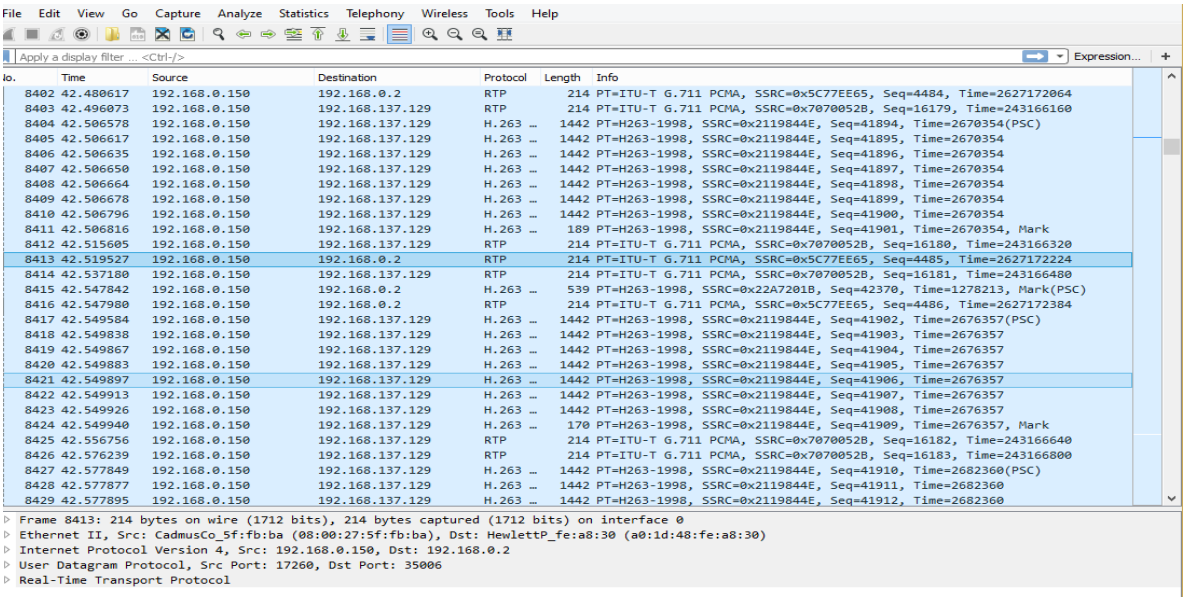


Figura 18- 3 Protocolo RTP y códec de video

Realizado por: Crow. W 2016

3.8 Parámetros a evaluar

Los parámetros que se evaluaron para definir la calidad de servicio que se obtuvo en la red mpls montada sobre equipos cisco 2900 al transferir audio y video son:

Perdida de paquetes:

Se produce Cuando varios paquetes de datos viajan por una red de un punto a otro y estos no son entregados o no llegan a su destino a tiempo son descartados lo cual desencadena en errores al momento de distinguir una comunicación. Valores máximos de perdida de paquetes recomendados por la UIT-T G.1010, Y.1541, IEEE 802.1p, para voz y video en tiempo real es de (1% a 3%).

Latencia o retardo:

En resumen es el tiempo que tarda el paquete de llegar del origen al destino o mejor conocido como la velocidad de transferencia de los datos. Valores máximos recomendados por La UIT-T G.1010, Y.1541, IEEE 802.1p, para voz y video sensible al retardo en tiempo real es de (100 a 150) ms.

Jitter:

Variación en el tiempo al llegar los paquetes de datos, esto es provocado por la saturación de la red acrecentando el retraso de la señal obteniendo un ruido no deseado. Valores máximos recomendados por la UIT-T G.1010, Y.1541, IEEE 802.1p, para voz y video en tiempo real es de (45 a 50) ms.

3.9 Resultados de los parámetros capturados de voz y video

3.9.1 Resultados de los parámetros al realizar una llamada de voip

Se procedió hacer la captura de los parámetros descritos en el apartado anterior al realizar una llamada voip entre los usuarios (100-101) utilizando el códec G.711 el cual no produce ruido por tal motivo el valor de jitter será muy bajo. Además la captura se la realizo mientras se inyectaba un tráfico externo con el programa Ostinato.

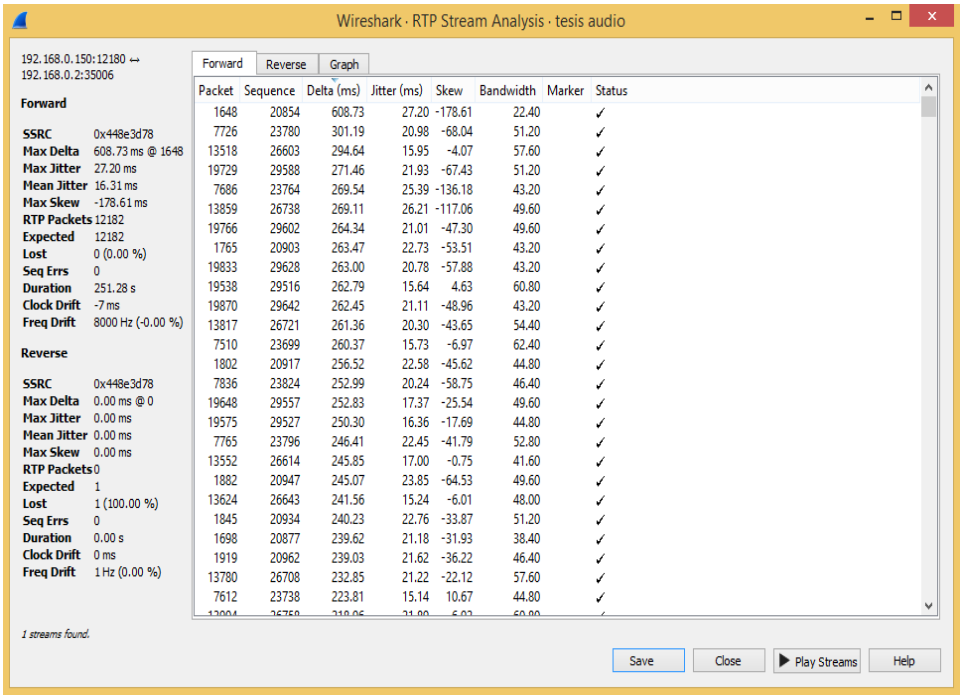


Figura 19- 3: Parámetros

Realizado por: Crow. W 2016

Se observa en la fig.19-3 un jitter máximo de 27.70 ms, la máxima latencia que se obtuvo fue de 608.73ms este incremento de la latencia comparando con los valores máximos recomendados es elevado debido a que el usuario 101 se lo conecto a la red a través de un router AP considerando que en entornos Wireless existe retardo a diferencia de una conexión por cable además la latencia máxima es un tiempo mínimo determinado, no hubo pérdidas de paquetes.

3.9.2 Resultados de los parámetros al realizar una video- llamada

Se realizó la captura de los parámetros ya establecidos al hacer video-llamada entre los usuarios (100-101) utilizando el códec de video H.263P. La captura se hizo mientras se inyectaba un tráfico externo.

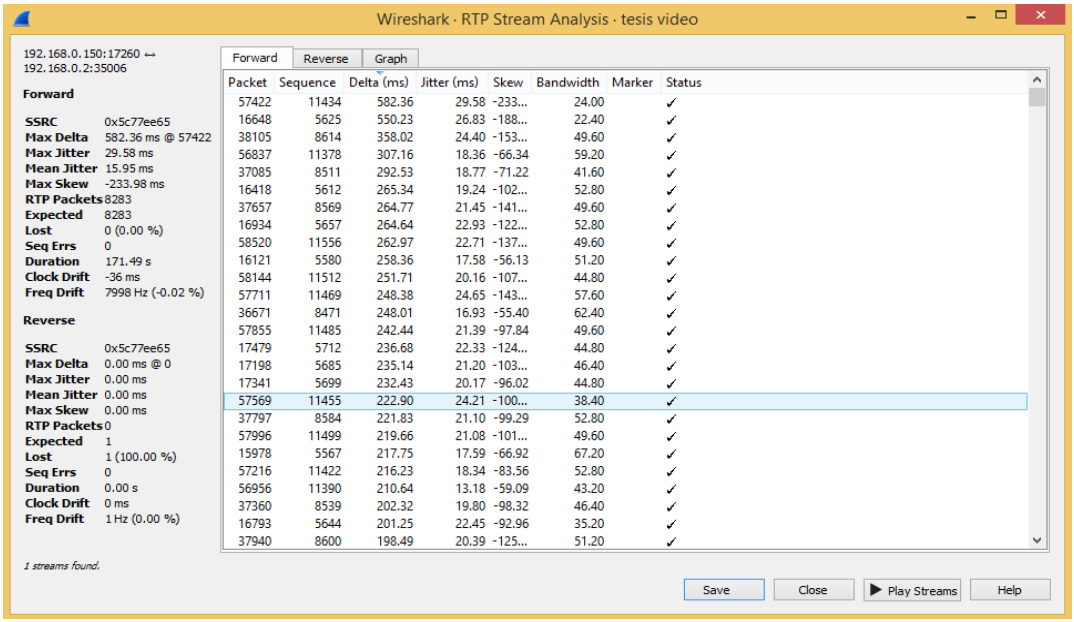


Figura 20- 3: Paquetes Wireshark

Fuente: Crow. W 2016

Se observa en la fig.20-3 un jitter máximo de 29.58 ms, la máxima latencia que se obtuvo fue de 582.36ms la explicación del incremento de la latencia es la misma que para voip, no hubo pérdidas de paquetes.

3.10 Evaluación de los parámetros obtenidos de voz y video

Para este apartado se determinó de una manera cuantitativa y cualitativa el cómo se va a evaluar los parámetros obtenidos. En la tabla 1-3 observamos las escalas cuantitativas y cualitativas con la que se evaluaran los resultados.

Tabla 1-3: Escala cuantitativas y cualitativas

Escala cuantitativa				
0	**1**	**2**	**3**	**4**
0%	**25%**	**50%**	**75%**	**100%**
Escala cualitativa				
Muy deficiente	**deficiente**	**Poco eficiente**	**Eficiente**	**Muy eficiente**

Realizado por: CROW, W, 2016

Fuente: RUBIO, M, 2010, p.18-20

Con esta tabla se describe la manera con la que los parámetros obtenidos se evaluaran a través de las capturas de los resultados de la llamada de voz y video durante las pruebas realizadas con los valores máximos recomendados por la UIT-T G.1010, Y.1541, IEEE 802.1p con referente al jitter, retardo o latencia, perdida de paquetes, utilizando ponderaciones.

3.10.1 Evaluación de los parámetros obtenidos de voz

En la tabla 2-3 se muestra los parámetros que se an obtenido. Comparando con los parámetros máximos recomendados por la UIT-T G.1010, Y.1541, IEEE 802.1p.

Tabla 2-3: Parámetros obtenidos y recomendados

Parámetros	UIT-T G.1010, Y.1541, IEEE 802.1p	Valores obtenidos
Jitter	50ms	27.70ms
Latencia	150ms	608.13ms
Perdida de paquetes	3%	0%

Realizado por: CROW.W, 2016

Fuente: BUÑAY, P, 2013, p.75, 78, 82

Luego Se procedió a realizar la tabla de ponderaciones en base a los resultados máximos recomendados de la UIT-T G.1010, Y.1541, IEEE 802.1p y los valores propios que se an obtenido al hacer el tráfico de voz en una red MPLS haciendo uso de las vrf tanto para tráfico externo y de voz para aislar el tráfico y obtener un mejor balanceo de carga.

Tabla 3-3: Ponderaciones

Parámetros	UIT-T G.1010, Y.1541, IEEE 802.1p	Valores obtenidos
Jitter	2	3
Latencia	3	1
Perdida de paquetes	1	4
Total	6	8
porcentaje	50%	66,66%

Realizado por: CROW, W, 2016

El valor de jitter=27.70ms el mismo que se encuentra dentro de los parámetros establecidos en la UIT-T G.1010, Y.1541, IEEE 802.1p y como se acerca más a 0 se considera que fue eficiente, el valor de la latencia=608.13ms supero al valor máximo recomendado por tal motivo se considera deficiente y como no hubo perdida de paquetes su ponderación fue muy eficiente. Para calcular el porcentaje se hizo uso de la siguiente formula:

$$P = \frac{\sum_1^5 V_i * 100\%}{T_i}$$

En la cual se realizó una evaluación global de todos los parámetros para comparar en base a porcentaje los valores que se obtuvo con los valores máximos recomendados por la UIT-T G.1010, Y.1541, IEEE 802.1p. En lo cual se calculó el total de la suma de las ponderaciones de los parámetros a evaluar, multiplicando con por 100 y dividendo para 12 que sería el valor máximo obtenido si cada para metro recibía una ponderación de 4 (muy satisfactorio) equivalente al 100%. En la figura 21-3 se puede observar el grafico de los porcentajes observando que nuestra arquitectura tiene un aumento de porcentaje en la calidad de servicio de 16.66% con la implementación que se hizo de MPLS utilizando sesiones BGP y creando vrf a través de MP-BGP. Esto con referencia a los valores de la UIT-T G.1010, Y.1541, IEEE 802.1p.

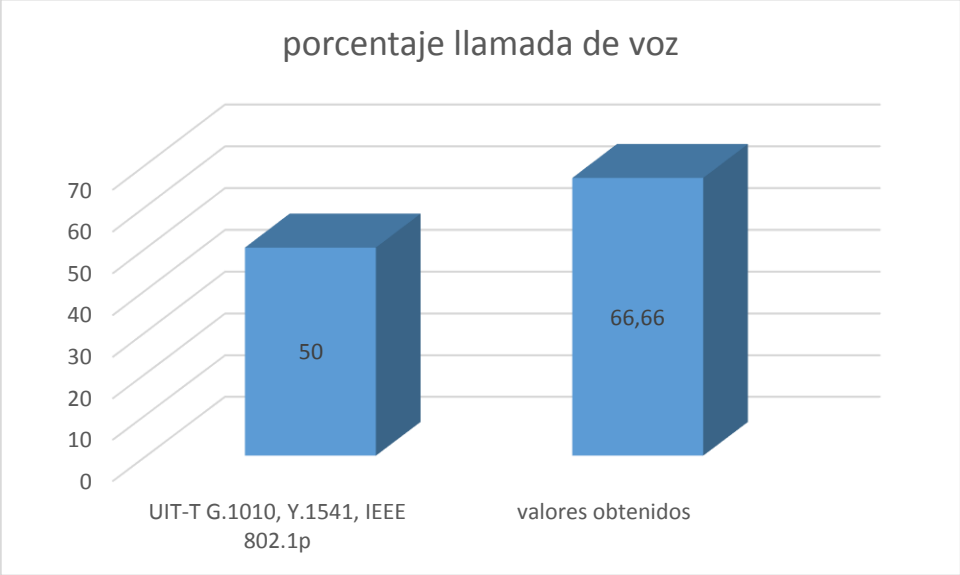


Figura 21-3: porcentaje del análisis de voz

Realizado por: CROW, W, 2016

3.10.2 Evaluación de los parámetros obtenidos en video llamada

Se determinó de la misma manera cualitativa y cuantitativa el cómo se evaluaría los parámetros. En la tabla 4-3 se evidencia resultados a ser ponderados.

Tabla 4-3: Parámetros a evaluar video llamada

Parámetros	UIT-T G.1010, Y.1541, IEEE 802.1p	Valores obtenidos
Jitter	50ms	29.58ms
Latencia	150ms	582.36ms
Perdida de paquetes	3%	0%

Realizado por: CROW, W, 2016

Se observa los resultados obtenidos de la llamada de video comparando con los valores máximos recomendados por la UIT-T G.1010, Y.1541, IEEE 802.1p. Luego se realizó las ponderaciones al igual que en la evaluación de voz con la diferencia que al ser video hizo uso del códec H.263P necesitando un mayor ancho de banda. En la tabla 5-3 se visualiza las ponderaciones para video.

Tabla 5-3: Ponderaciones del análisis de video llamada

parámetros	UIT-T G.1010, Y.1541, IEEE 802.1p	Valores obtenidos
Jitter	2	3
Latencia	3	1
Perdida de paquetes	1	4
Total	6	8
porcentaje	50%	66,66%

Realizado por: CROW, W, 2016

El valor de jitter=29.58ms obtuvo un aumento mínimo con referencia al resultado de voz aunque se encuentra dentro de los parámetros establecidos en la UIT-T G.1010, Y.1541, IEEE 802.1p y como se acerca más a 0 se considera que fue eficiente, el valor de la latencia=582.36.13ms disminuyó referente al resultado de voz pero su incremento supero al valor máximo recomendado por tal motivo se considera deficiente y como no hubo perdida de paquetes su ponderación fue muy eficiente. Para calcular el porcentaje se usó la misma fórmula que en la evaluación de voz:

$$P = \frac{\sum_1^5 V_i * 100\%}{T_i}$$

Se realizó una evaluación global de todos los parámetros para comparar en base a porcentaje los valores que se obtuvo, con los valores máximos recomendados por la UIT-T G.1010, Y.1541, IEEE 802.1p. De esta manera se podría establecer si el sistema implementado tendría mejoras. La manera de reemplazar los valores ponderados es la misma que la evaluación de voz. Por último se realizó un gráfico donde se observa los porcentaje obtenidos de entre los valores de la UIT-T G.1010, Y.1541, IEEE 802.1p, y los valores que se obtuvieron de las pruebas realizadas en la arquitectura de red MPLS y VRF creadas con el protocolo MP-BGP familia de BGP. Ofreciendo un aumento en el análisis global de sus parámetros de calidad en 16,66% en referencia a los valores máximos permitidos.

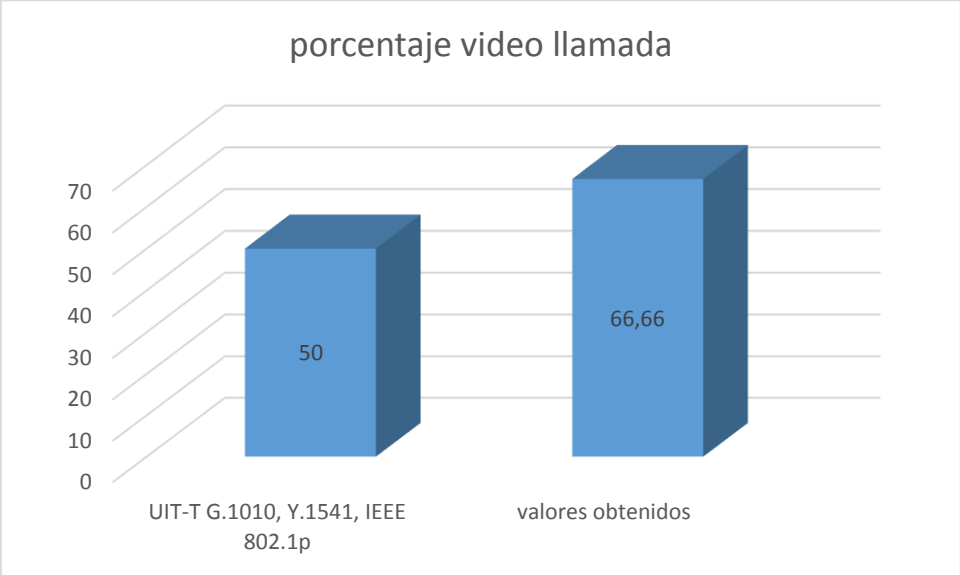


Figura 22-3: porcentaje de la evaluación de video

Realizado por:

3.11 Consideraciones en base a los resultados

En este apartado se proponen condiciones mínimas que se requieren para implementar una red mpls que asegure la QoS basándose en los resultados obtenidos durante el desarrollo del presente trabajo de titulación.

3.11.1 Características de los equipos

Para el desarrollo del trabajo presentado se hizo uso de equipos CISCO 2900 el cual presentaba las condiciones necesarias para implementar el sistema, por lo cual se recomienda utilizar estos equipos o equipos de mejor gama siempre y cuando como mínimo cumplan con el soporte de los siguientes protocolos:

- Enrutamiento dinámico
- Soporte del protocolo MPLS
- Protocolo BGP
- MP-BPG familia de BGP

Además para la parte del servidor Elastix contar con un equipo con alta velocidad de procesamiento como las que posee los ordenadores de última generación, este requerimiento varía dependiendo de las necesidades que se requiera cumplir.

Para la conexión de equipos móviles dentro de la topología de red es necesario de un router AP que brinde el alcance suficiente para permitir la comunicación a larga distancia sin perdidas de conexión. Además se podría considerar hacer uso de un router Wireless con soporte multimedia el cual brinde una mejor calidad de servicio y priorice las aplicaciones en tiempo real.

3.11.2 Consideraciones a nivel de software

Con respecto al software se puede tomar en cuenta el empleo de herramientas con licencia ya que algunos de estos proporcionan servicios adicionales con respecto al software libre como por ejemplo el servidor elastix.

Durante el desarrollo del presente trabajo se observó que es necesario que el códec de audio y video tanto en el servidor como en los usuarios debe ser el mismo con el fin de evitar errores al realizar una

llamada o video llamada. Del mismo modo que con elastix se recomienda utilizar codecs licenciados que brinden mayor compresión sin deteriorar la calidad de la voz y video y permita usar un menor ancho de banda con lo cual se evitara un desperdicio de recursos.

3.11.3 Consideraciones de QoS a partir de los resultados obtenidos

Una vez cumplidos los requerimientos antes mencionados se estima un rango de parámetros en base a los resultados obtenidos conociendo que la topología implementada tuvo un mejoramiento global del 10.66% tanto para audio y video en referencia a los valores máximos permitidos.

En relación al jitter se recomienda un rango de funcionamiento entre (27 a 30) ms, con respecto a los paquetes perdidos cuando su porcentaje sea más aproximado a cero se considera eficiente o cero muy eficiente, por último la latencia mientras se tome en cuenta los requerimientos ya mencionados en los apartados anteriores y así evitar el congestionamiento de la red siempre se obtener un resultado muy por debajo del límite máximo permitido.

En este trabajo se obtuvo un valor de latencia máxima en un tiempo mínimo determinado por encima del límite esto se debe a que no se pudo acceder a un router AP multimedia. Al tomar en cuenta la evaluación en conjunto de los 3 parámetros se mejoró en base a los límites permitidos.

CONCLUSIONES

- Partiendo de un estudio se conoció el proceso de empaquetamiento y distribución del protocolo MPLS, de esta manera tiene la necesidad de utilizar de un protocolo que brinde conectividad como por ejemplo OSPF. Además para brindar mejores condiciones a la arquitectura de red era necesario del uso del protocolo BGP para establecer un enlace entre routers servidor-cliente y MP-BGP para la creación de las vrf de esta manera obtener un mejor balanceo de carga al tener aislado el tráfico.

- Se implementó la red MPLS mediante el uso de equipos CISCO que primero fue emulado en GNS3 para posterior inyectar un tráfico externo a través de la respectiva vrf (trafico) se logró capturar datos de voz y video en condiciones las cuales para el análisis de calidad de servicio (jitter, retardo, perdida de paquetes) no podían ser ideales al contrario lo que se buscó al ingresar este tráfico era analizar los paquetes en condiciones reales, de esta manera se visualizó su comportamiento a través del wireshark .

- Las pruebas realizadas en los laboratorios cisco de la Escuela Superior Politécnica de Chimborazo demostró un 66,66% en el trafico tanto para voz y video a consideración del 50% de los valores máximos recomendados por la UIT-T G.1010, Y.1541, IEEE 802.1p, concluyendo que se obtuvo una mejora del 16,66% con la arquitectura de red MPLS utilizando VRF para aislar el tráfico de tiempo real con el trafico externo que este caso fue TCP lo cual demostró un nivel eficiente en la evaluación comparando con los valores máximos recomendados UIT-T G.1010, Y.1541, IEEE 802.1p.

- La tecnología de las telecomunicaciones evolucionan constantemente es por eso que cada vez existen nuevas y mejores maneras de asegurar la calidad de servicio y más aún en aplicaciones de audio y video. Lo cual se propone investigar sobre IGMPLS que son redes de fibra óptica. Redes con servicios diferenciados que den prioridad a los paquetes más críticos como los de en tiempo real.

RECOMENDACIONES

- Para diseñar y crear una red MPLS se debe conocer a exactitud cuál es su funcionamiento, los comandos necesarios para implementar la arquitectura.

- Hay que probar la topología de red su funcionamiento y convergencia de acuerdo a las necesidades que tengamos haciendo uso de algún emulador ya que comprobando que existe comunicación se puede pasar a la siguiente etapa que es configurar en los equipos físicos con la seguridad de que deberá converger.

- Si se quiere tener una calidad mejor de servicio con los equipos y materiales que me lo permita es de vital importancia realizar investigación para poner realizar las pruebas partiendo de estudios ya empleados.

- Se aconseja revisar que los equipos cisco funcionen correctamente además de los cables seriales y cables directos para no tener problemas de hardware al configurar o establecer conexión.

- Se recomienda considerar que al utilizar una conexión a través de un router AP existen retardos al conectar equipos móviles por el motivo de interrupciones externas del ambiente donde se realice las pruebas.

BIBLIOGRAFIA

- **ABDELALI, *A*** *Essaaidi, Using LDP Fastreroute versus LDP o RSVP in an MPLS core backbone for convergence enhancement, J.Theoretical and Applied Information Technolog* [En línea] 2013 Chile [Consulta:2 de Abril del 2016] disponible en: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642014000200004

- **AFARREL , Ernesto** *Big Book of MPLS (multiprotocol Label Switching)* [En línea] 2006 España [Consulta:2 de abril del 2016] disponible en: http://www.todotecnologia.net/wp-content/uploads/2010/06/Caracteristicas_definicion_MPLS_GMPLS_ASON.pdf

- **ALVAREZ,S** QoS for IP/MPLS Cisco Press [En línea] 2001 México [Consulta: 6 de abril del 2016] disponible en http://tools.ietf.org/html/rfc4301

- **AVALLONE, L** *An experimental analysis of Diffserv-MPLS interoperability* En línea] 2009 España [Consulta:2 de abril del 2016] disponible en: http://www.scielo.cl/pdf/infotec/v25n2/art04.pdf

- **BEHRINGER, M** *Generic Routing Encapsulation* [En línea] 2002 Venezuela [Consulta: 2 de abril del 2016] disponible en: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/prod_presentation0900aecd80311df4.pdf.

- **BEIJNUM, I** *Multiprotocol MPLS* [En línea] 2012 España [Consulta: 6 de abril del 2016] disponible en: http://MPLS.uach.cl//uach/2012/bmfcic828r/sources/bmfcic828r.pdf

- **BRENDAN H** *Comunicaciones Unificadas con Elastix* [En línea] 2013 Estados Unidos Consulta: 2 de abril del 2016] disponible en: http://www.ebook3000.com/Practical-Raspberry-Pi_195870.html.

- **BUSTOS, Manuel** *Elastix* [En línea] 2013 [Consulta:2 de abril del 2016] disponible en: http://www.voipforo.com/codec/codecs.php

- **DAMON, Wischik** *Introducción a las tecnologías MPLS y GMPLS* [En línea] 2000 España [Consulta:3 de abril del 2016] disponible en http://www.ietf.org/rfc/rfc3945.txt

- **DEERING, S** *Framework for QoS-based Routing* [En línea] 2002 México [Consulta: 7 de abril del 2016] disponible en: http://faizalrahimi.wordpress.com/

- **DEERING, DEPLOYING** *IP and MPLS QoS for Multiservice* [En línea] 2003 USA [Consulta: 7 de abril del 2016] disponible en: www.grid.unina.it/software/ITG.

- **ENRIQUEZ, S** *Traffic Engineering with MPLS* [En línea] 2008 Colombia [Consulta:5 de abril del 2016] disponible en: http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/prodlit/iosmp_ai.pdf

- **EVANS, J** *Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP)* [En línea] 2008 USA [Consulta: 6 de abril del 2016] disponible en: http://www.ietf.org/rfc/rfc2547.txt

- **GALLEAR, T** *Software and Multiprotocol Label Switching* [En línea] 2003 México [Consulta: 5 de abril del 2016] disponible en: http://www.ietf.org/internet-drafts/draft-martiniethernet-encap-mpls-02.txt

- **GALLAHER, RICK** *MPLS Training Guide Building Multi Protocol Label Switching* [En línea] 2006 España [Consulta: 10 de abril del 2016] disponible en: www.info-ab.uclm.es/sec-ab/Tecrep/diab-01-02-16.pdf

- **GALVEZ,L** *MPLS y sus Componentes* [En línea] 2002 España [Consulta: 5 de abril del 2016] disponible en: http://ldc.usb.ve/~poc/RedesII/Grupos/G5/mpls_y_sus_componentes.htm

- **GAVALANEZ Malkin** *VoIP QoS requirements* [En línea] 2009 México [Consulta: 5 de abril del 2016] disponible en: http://www.voipinfo.org/wiki/view/QoS

- **GREOSSETETE.*P*** *On the difficulty of establishing interdomain LSPs. Proceedings of the IEEE Workshop on IP Operations and Management* [En línea] 2001 USA [Consulta : 6 de

Abril del 2016] Disponible en: http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html

- **HARNEDY, L** *QoS routing mechanisms and OSPF extensions* [En línea] 2011 España [Consulta: 6 de abril del 2016] Disponible en: http://www.infcr.uclm.es/www/edguez/rap_0506/Transparencias/ATM

- **HESSELBACH, Xavier** *Arquitectura MPLS MPLS* [En línea] 2010 México [Consulta: 10 de abril del 2016] disponible en: http://www.juniper.net/solutions/literature/white_papers/200160.pdf

- **JAEGER, Juniper** *Enhancing Routing in the New Public Network* [En línea] 2007 Bogotá [Consulta:7 de abril del 2016] disponible en web: http://www.laccei.org/LACCEI2007-Cartagena/Papers/IT083.pdf

- **JARRIN A** *Redes MPLS fundamentos, aplicación y gestión de recursos* [En línea] 2001 Brazil [Consulta: 8 de abril del 2016] disponible en: http://www.todotecnologia.net/wp-content/uploads/2010/06/Caracteristicas_definicion_MPLS_GMPLS_ASON.pdf

- **KUMAKI, L** *Una arquitectura de backbone para la Internet del siglo XXI* [En línea] 2008 Venezuela [Consulta: 9 de abril del 2016] disponible en: http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html

- **KODIALAM, M** *QoS Routing. IEEE Communications Magazine* [En línea] 2009 México [Consulta: 9 de abril del 2016] disponible en: http://www.cisco.com/warp/public/cc/so/neso/vvda/ipatm/mpls_wp.htm

- **LANDIVAR, M** *Seguridad en implementaciones de voz sobre IP* [En línea] 2011 Estados Unidos [Consulta: 10 de abril del 2016] disponible en: http://www.elastix.org/index.php/es/informacion-del-producto/manualeslibros.html#sivoipi

- **LLOYD**, **Robert** *Medición de la Calidad del Servicio* [En línea] 2001 México [Consulta: 5 de abril del 2016] disponible en: http://conecta-wireless.com/conectividad/redes-privadas-vpn-independientes-y- seguras?view=

- **LOSHIN, *Peter*** *Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS)* [En línea] 2008 USA [Consulta: 10 de abril del 2016] disponible en: http://www.cisco.com/warp/public/cc/so/neso/vpn/vpnsp/ievpn_rg.htm

- **MARQUES, P** *Overview and Principles of Internet Traffic Engineering* [En línea] 2005 Canadá [Consulta: 8 de abril del 2016] disponible en: http://www.upcommons.upc.edu/pfc/bitstream/2099.1/8773/1/Proyecto%20 PCE.pdf.

- **OLIVA, J** *Software PBX Elastix* [En línea] 2011 España [Consulta: 5 de abril del 2016] disponible en: http://www.alsa-project.org/main/index.php/Main

- **OSBORNE,E** *Traffic Engineering with MPLS* [En línea] 2002 Chile [Consulta: 5 de abril del 2016] disponible en: http://dspace.uclv.edu.cu/bitstream/handle/123456789/4832/Aliemnis%20Reinier%20Beltr%C3%A1n%20Arbol%C3%A1ez.pdf?sequence=1&isAllowed=y

- **PICO, J** *Configuración de QoS* [En línea] 2009 España [Consulta: 7 de abril del 2016] disponible en: http://www.ub.edu.ar/investigaciones/tesinas/259

- **REDFORD, Rob** *Signaling Extensions for MPLS Traffic Engineering* [En línea] 2004 Canadá [Consulta: 5 de abril del 2016] disponible en: http://www.ietf.org/html.charters/mpls-charter.html

- **REKHTER, *Y*** *The Evolution of MPL [*En línea] 2006 México [Consulta: 10 de abril del 2016] disponible en: http://faizalrahimi.wordpress.com/

- **ROBERTSON, W** *An Architecture for Differentiated Services MPLS* [En línea] 2006 Canadá [Consulta: 10 de Abril del 2016] disponible en: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_d_l/capitulo2.pdf

- **ROSEN E** *Multiprotocol Label Switching Architecture* [En línea] 2008 Inglaterra [Consulta: 6 de abril del 2016] disponible en: http://www.iec.org/online/tutorials/mpls.

- **SATISH, Jamadagni** *Scalability Considerations in BGP/MPLS IP* [En línea] 2001 USA [Consulta: 9 de abril del 2016] disponible en: http://www.ietf.org/internet-drafts/draftkompella-l2vpn-l2vpn-01.tx

- **SRISURESH, Y** *Calidad de servicio en IPv6* [En línea] 2006 México [Consulta: 9 de abril del 2016] disponible en: http://www.redes-MPLS .com/manualesQos.

- **THOMAS G** *QoS in Integrated MPLS* [En línea] 2005 Canadá [Consulta: 10 de abril del 2016] disponible en: http://www.ipv6-tf. com.pt/implementacoes/files/cisco/ipv6_. erconnectingIPv6DomainsUsingTunnels. Pdf

- **VILALTA,E** *Multi-protocol label switching (MPLS) support of differentiated services* [En línea] 2012 Chile [Consulta: 10 de abril del 2016] disponible en http://www.scielo.cl/pdf/infotec/v25n2/art04.pdf

ANEXOS

ANEXO A. Configuración de los routers

PE-1

```
PE-1(config)#router ospf 1
PE-1(config-router)#network 172.30.1.0 0.0.0.255 area 0
PE-1(config-router)#network 172.30.5.0 0.0.0.3 area 0
PE-1(config-router)#network 172.30.5.12 0.0.0.3 area 0
PE-1(config)#ip cef
PE-1(config)#mpls label protocol ldp
PE-1(config)#mpls ip
PE-1(config)#interface serial 0/0
PE-1(config-if)#mpls label protocol ldp
PE-1(config-if)#mpls ip
PE-1(config-if)#exit
PE-1(config)#interface serial 0/1
PE-1(config-if)#mpls label protocol ldp
PE-1(config-if)#mpls ip
PE-1(config-if)#exit
PE-1(config)#router bgp 1
PE-1(config-router)#no auto-summary
PE-1(config-router)#no synchronization
PE-1(config-router)#neighbor 172.30.3.1 remote-as 1
PE-1(config-router)#neighbor 172.30.3.1 update-source loopback 0
PE-1(config-router)#address-family vpnv4
PE-1(config-router-af)#neighbor 172.30.3.1 activate
PE-1(config-router-af)#neighbor 172.30.3.1 send-community extended
PE-1(config-router-af)#exit
PE-1(config)#ip vrf voip
PE-1(config-vrf)#rd
PE-1(config-vrf)#rd 1:1
PE-1(config-vrf)#route-target 1:1
PE-2(config-vrf)#exit
PE-1(config)#ip vrf trafico
PE-1(config-vrf)#rd 1:2
PE-1(config-vrf)#route-target 1:2
```

```
PE-1(config-vrf)#exit
PE-1(config)#interface fastEthernet 0/1
PE-1(config-if)#ip vrf forwarding voip
PE-1(config-if)#ip address 192.168.1.1 255.255.255.0
PE-1(config-if)#mpls label protocol ldp
PE-1(config-if)#mpls ip
PE-1(config-if)#exit
PE-1(config)#router bgp 1
PE-1(config-router)#address-family ipv4 vrf voip
PE-1(config-router-af)#redistribute connected
PE-1(config-router-af)#no synchronization
PE-1(config-router-af)#exit-address-family
PE-1(config-router)#exit
PE-1(config)#interface fastEthernet 0/0
PE-1(config-if)#ip vrf forwarding trafico
PE-1(config-if)#ip address 192.168.3.1 255.255.255.0
PE-1(config-if)#mpls label protocol ldp
PE-1(config-if)#mpls ip
PE-1(config-if)#exit
PE-1(config)#router bgp 1
PE-1(config-router)#address-family ipv4 vrf trafico
PE-1(config-router-af)#redistribute connected
PE-1(config-router-af)#no synchronization
PE-1(config-router-af)#exit-address-family
PE-1(config-router)#exit
```

```
P-1
Router>enable
Router#conf t
Router(config)#hostname P-1
P-1(config)#interface loopback 0
```

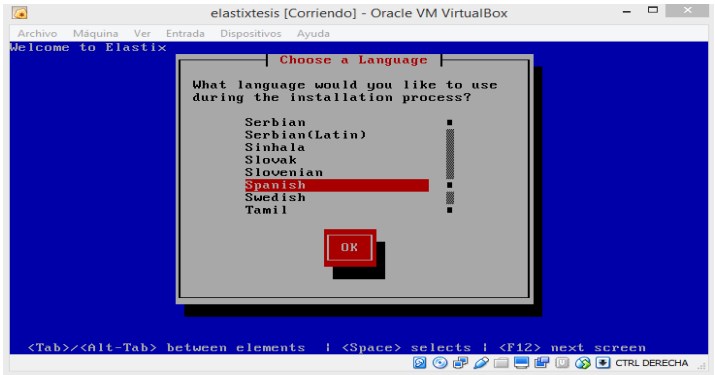
```
P-1(config-if)#ip address 172.30.2.1 255.255.255.0
P-1(config-if)#interface serial 0/0
P-1(config-if)#ip address 172.30.5.2 255.255.255.252
P-1(config-if)#no sh
P-1(config-if)#interface serial 0/1
P-1(config-if)#ip address 172.30.5.5 255.255.255.252
P-1(config-if)#no sh
P-1(config-if)#exit
P-1(config)#router ospf 1
P-1(config-router)#network 172.30.2.0 0.0.0.255 area 0
P-1(config-router)#network 172.30.5.0 0.0.0.3 area 0
P-1(config-router)#network 172.30.5.4 0.0.0.3 area 0
P-1(config-router)#exit
P-1(config)#ip cef
P-1(config)#mpls label protocol ldp
P-1(config)#mpls ip
P-1(config)#interface serial 0/0
P-1(config-if)#mpls label protocol ldp
P-1(config-if)#mpls ip
P-1(config-if)#exit
P-1(config)#interface serial 0/1
P-1(config-if)#mpls label protocol ldp
P-1(config-if)#mpls ip
P-1(config-if)#exit

PE-2
router ospf 1
network 172.30.3.0 0.0.0.255 area 0
network 172.30.5.4 0.0.0.3 area 0
network 172.30.5.8 0.0.0.3 area 0
PE-2(config)#ip cef
PE-2(config)#mpls label protocol ldp
PE-2(config)#mpls ip
PE-2(config)#interface serial 0/0
```

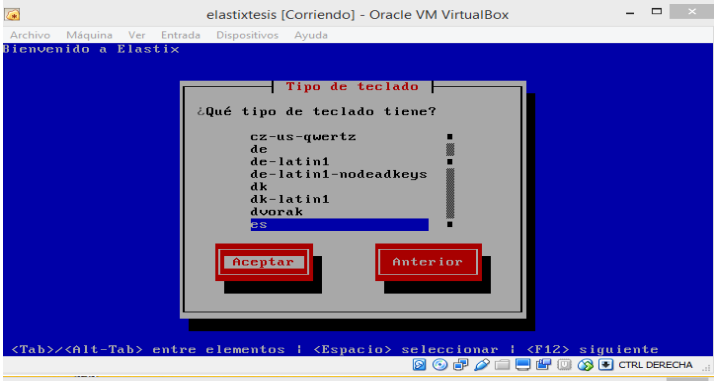
```
PE-2(config-if)#mpls label protocol ldp
PE-2(config-if)#mpls ip
PE-2(config-if)#exit
PE-2(config)#interface serial 0/1
PE-2(config-if)#mpls label protocol ldp
PE-2(config-if)#mpls ip
PE-2(config-if)#exit
PE-2(config)#router bgp 1
PE-2(config-router)#no auto-summary
PE-2(config-router)#no synchronization
PE-2(config-router)#neighbor 172.30.1.1 remote-as 1
PE-2(config-router)#neighbor 172.30.1.1 update-source loopback 0
PE-2(config-router)#address-family vpnv4
PE-2(config-router-af)#neighbor 172.30.1.1 activate
PE-2(config-router-af)#neighbor 172.30.1.1 send-community extended
PE-2(config-router-af)#exit
PE-2(config)#ip vrf voip
PE-2(config-vrf)#rd
PE-2(config-vrf)#rd 1:1
PE-2(config-vrf)#route-target 1:1
PE-2(config-vrf)#exit
PE-2(config)#ip vrf trafico
PE-2(config-vrf)#rd 1:2
PE-2(config-vrf)#route-target 1:2
PE-2(config-vrf)#exit
PE-2(config)#interface fastEthernet 0/1
PE-2(config-if)#ip vrf forwarding voip
PE-2(config-if)#ip address 192.168.2.1 255.255.255.0
PE-2(config-if)#mpls label protocol ldp
PE-2(config-if)#mpls ip
PE-2(config-if)#no sh
PE-2(config)#router bgp 1
PE-2(config-router)#address-family ipv4 vrf voip
PE-2(config-router-af)#redistribute connected
```

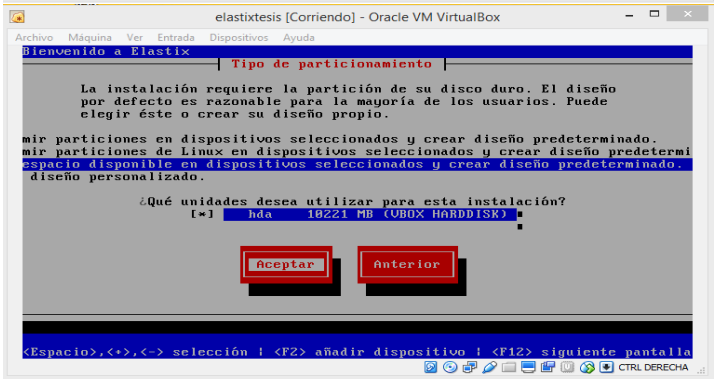
```
PE-2(config-router-af)#no synchronization
PE-2(config-router-af)#exit-address-family
PE-2(config-router)#exit
PE-2(config)#interface fastEthernet 0/0
PE-2(config-if)#ip vrf forwarding trafico
PE-2(config-if)#ip address 192.168.4.1 255.255.255.0
PE-2(config-if)#mpls label protocol ldp
PE-2(config-if)#mpls ip
PE-2(config-if)#exit
PE-2(config)#router bgp 1
PE-2(config-router)#address-family ipv4 vrf trafico
PE-2(config-router-af)#redistribute connected
PE-2(config-router-af)#no synchronization
PE-2(config-router-af)#exit-address-family
PE-2(config-router)#exit
```

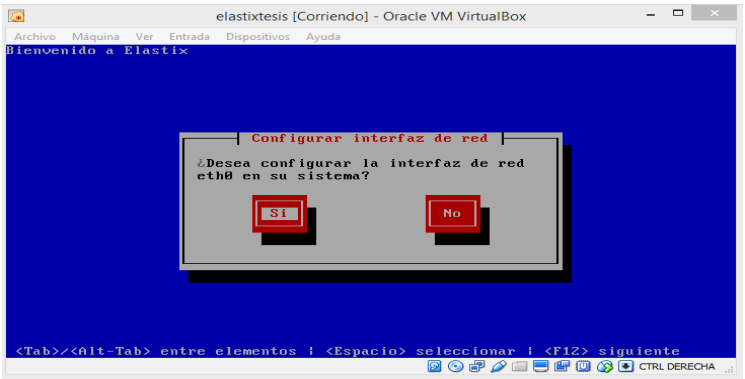
```
P-2
P-2#enable
P-2#conf t
P-2(config)#router ospf 1
P-2(config-router)#network 172.30.4.0 0.0.0.255 area 0
P-2(config-router)#network 172.30.5.8 0.0.0.3 area 0
P-2(config-router)#network 172.30.5.12 0.0.0.3 area 0
P-2(config-router)#exit
P-2(config)#ip cef
P-2(config)#mpls label protocol ldp
P-2(config)#mpls ip
P-2(config)#interface serial 0/0
P-2(config-if)#mpls label protocol ldp
P-2(config-if)#mpls ip
P-2(config-if)#exit
P-2(config)#interface serial 0/1
P-2(config-if)#mpls label protocol ldp

P-2(config-if)#mpls ip
P-2(config-if)#exit
```

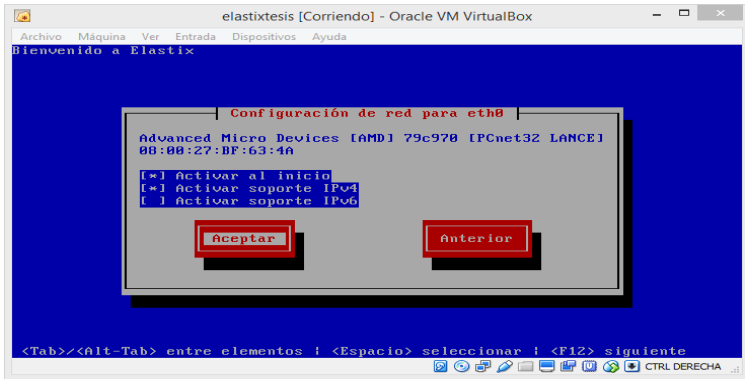
ANEXO B. Instalación Elastix

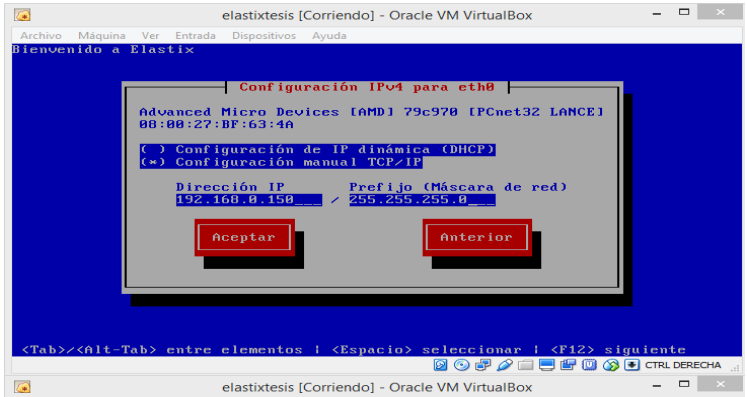


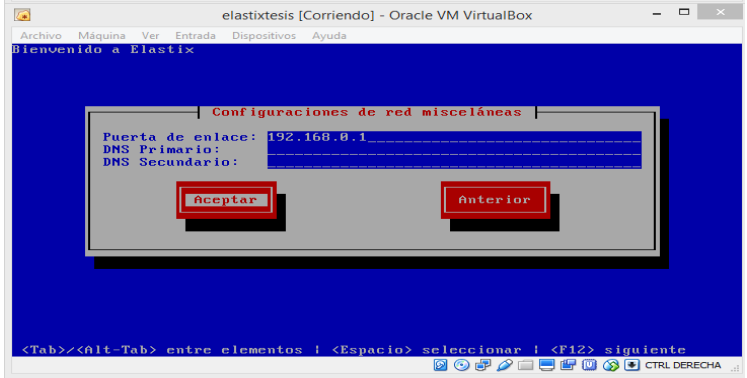


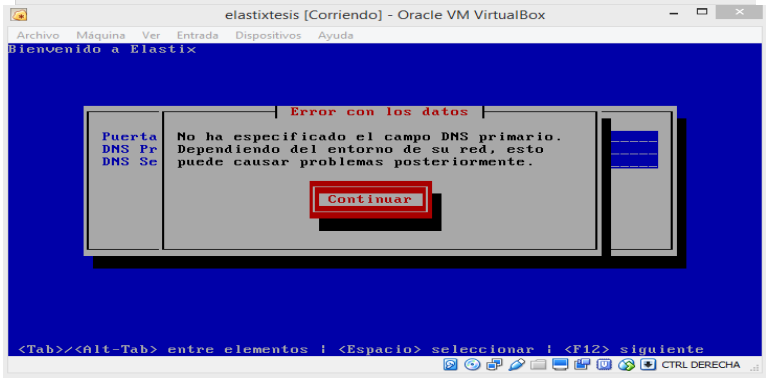


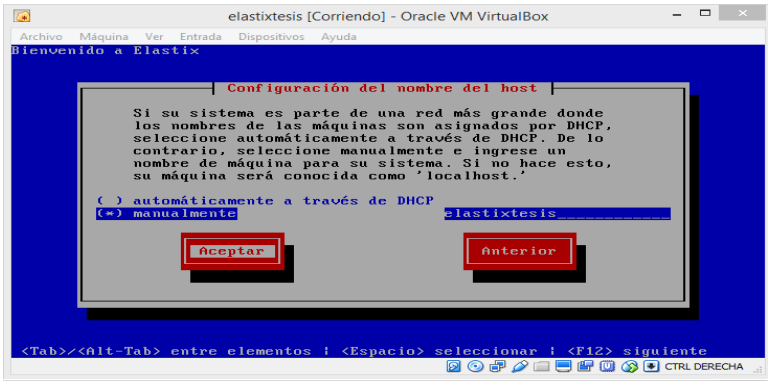


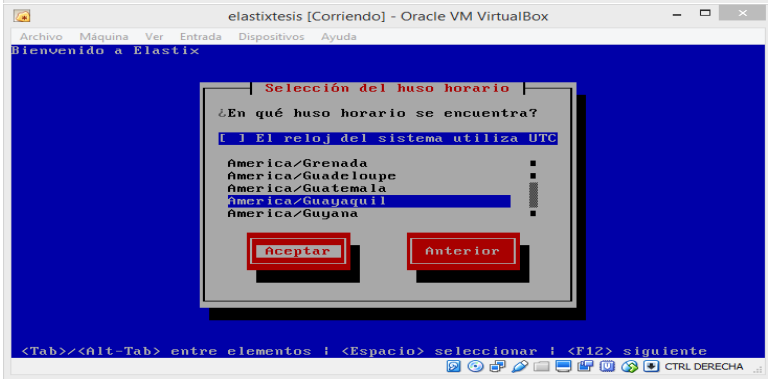

elastixtesis [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Bienvenido a Elastix
Configuración de red para eth0
Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
08:00:27:BF:63:4A
[*] Activar al inicio
[*] Activar soporte IPv4
[ ] Activar soporte IPv6
Aceptar
Anterior
<Tab>/<Alt-Tab> entre elementos | <Espacio> seleccionar | <F12> siguiente
CTRL DERECHA

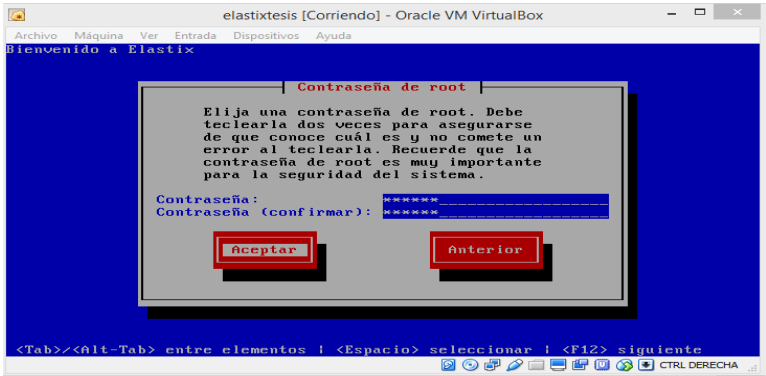

elastixtesis [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Bienvenido a Elastix
Configuración IPv4 para eth0
Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
08:00:27:BF:63:4A
( ) Configuración de IP dinámica (DHCP)
(*) Configuración manual TCP/IP
Dirección IP
Prefijo (Máscara de red)
192.168.0.150
255.255.255.0
Aceptar
Anterior
<Tab>/<Alt-Tab> entre elementos | <Espacio> seleccionar | <F12> siguiente
CTRL DERECHA

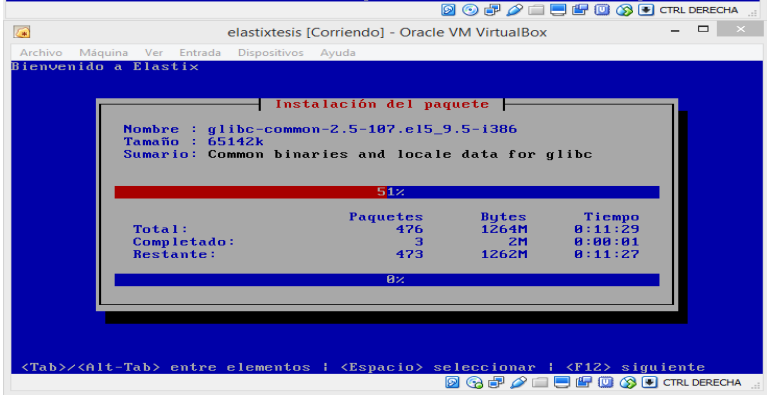

elastixtesis [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Bienvenido a Elastix
Configuraciones de red misceláneas
Puerta de enlace: 192.168.0.1
DNS Primario:
DNS Secundario:
Aceptar
Anterior
<Tab>/<Alt-Tab> entre elementos | <Espacio> seleccionar | <F12> siguiente
CTRL DERECHA

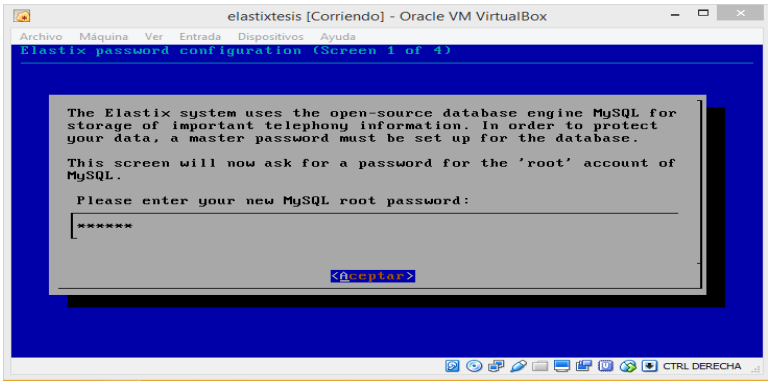

elastixtesis [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Bienvenido a Elastix
Error con los datos
Puerta
DNS Pr
DNS Se
No ha especificado el campo DNS primario.
Dependiendo del entorno de su red, esto
puede causar problemas posteriormente.
Continuar
<Tab>/<Alt-Tab> entre elementos | <Espacio> seleccionar | <F12> siguiente
CTRL DERECHA

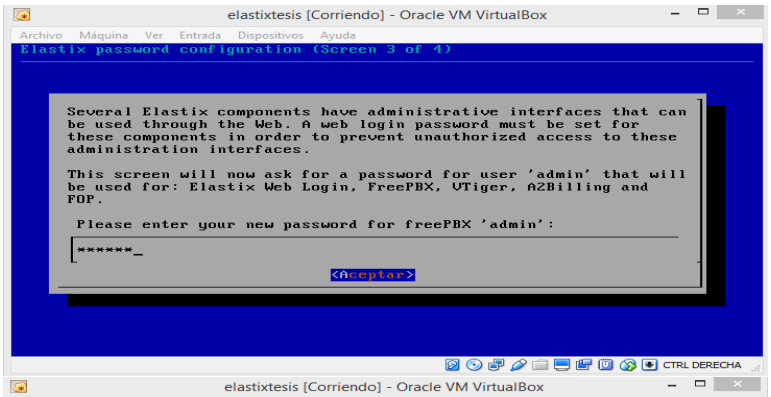

elastixtesis [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Bienvenido a Elastix
Configuración del nombre del host
Si su sistema es parte de una red más grande donde los nombres de las máquinas son asignados por DHCP, seleccione automáticamente a través de DHCP. De lo contrario, seleccione manualmente e ingrese un nombre de máquina para su sistema. Si no hace esto, su máquina será conocida como 'localhost.'
( ) automáticamente a través de DHCP
(*) manualmente
elastixtesis
Aceptar
Anterior
<Tab>/<Alt-Tab> entre elementos | <Espacio> seleccionar | <F12> siguiente
CTRL DERECHA

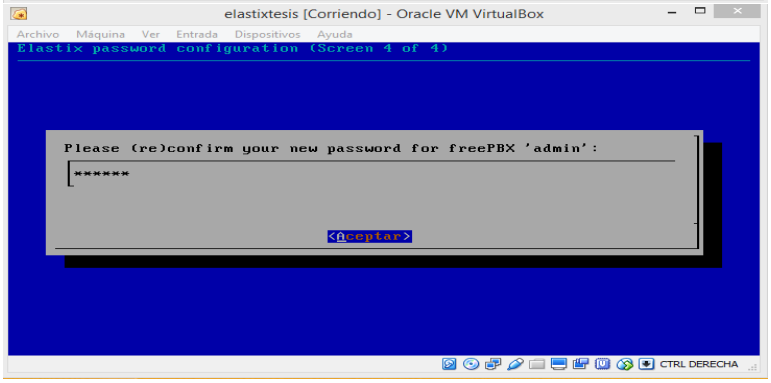

elastixtesis [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Bienvenido a Elastix
Selección del huso horario
¿En qué huso horario se encuentra?
[ ] El reloj del sistema utiliza UTC
America/Grenada
America/Guadeloupe
America/Guatemala
America/Guayaquil
America/Guyana
Aceptar
Anterior
<Tab>/<Alt-Tab> entre elementos | <Espacio> seleccionar | <F12> siguiente
CTRL DERECHA

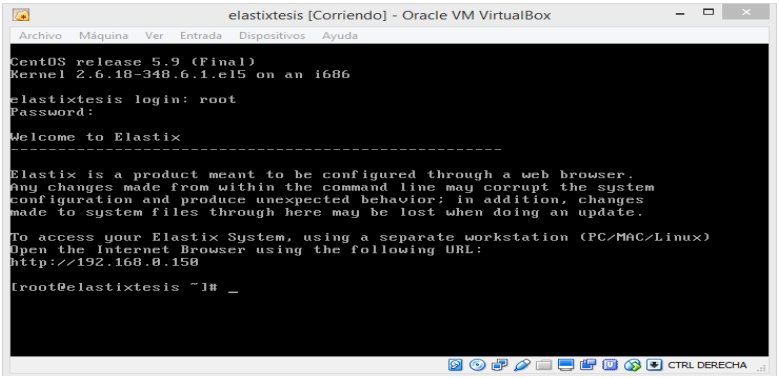

elastixtesis [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Bienvenido a Elastix
Contraseña de root
Elija una contraseña de root. Debe teclearla dos veces para asegurarse de que conoce cuál es y no comete un error al teclearla. Recuerde que la contraseña de root es muy importante para la seguridad del sistema.
Contraseña: ******
Contraseña (confirmar): ******
Aceptar
Anterior
<Tab>/<Alt-Tab> entre elementos | <Espacio> seleccionar | <F12> siguiente
CTRL DERECHA


elastixtesis [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Bienvenido a Elastix
Instalación del paquete
Nombre : glibc-common-2.5-107.el5_9.5-i386
Tamaño : 65142k
Sumario: Common binaries and locale data for glibc
51%
Paquetes Bytes Tiempo
Total: 476 1264M 0:11:29
Completado: 3 2M 0:00:01
Restante: 473 1262M 0:11:27
0%
<Tab>/<Alt-Tab> entre elementos | <Espacio> seleccionar | <F12> siguiente
CTRL DERECHA


elastixtesis [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Elastix password configuration (Screen 1 of 4)
The Elastix system uses the open-source database engine MySQL for storage of important telephony information. In order to protect your data, a master password must be set up for the database.
This screen will now ask for a password for the 'root' account of MySQL.
Please enter your new MySQL root password:
******
<Aceptar>
CTRL DERECHA


elastixtesis [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Elastix password configuration (Screen 3 of 4)
Several Elastix components have administrative interfaces that can be used through the Web. A web login password must be set for these components in order to prevent unauthorized access to these administration interfaces.
This screen will now ask for a password for user 'admin' that will be used for: Elastix Web Login, FreePBX, VTiger, A2Billing and FOP.
Please enter your new password for freePBX 'admin':
******
<Aceptar>
CTRL DERECHA


elastixtesis [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Elastix password configuration (Screen 4 of 4)
Please (re)confirm your new password for freePBX 'admin':
******
<Aceptar>
CTRL DERECHA


elastixtesis [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
CentOS release 5.9 (Final)
Kernel 2.6.18-348.6.1.el5 on an i686
elastixtesis login: root
Password:
Welcome to Elastix
Elastix is a product meant to be configured through a web browser.
Any changes made from within the command line may corrupt the system
configuration and produce unexpected behavior; in addition, changes
made to system files through here may be lost when doing an update.
To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://192.168.0.150
[root@elastixtesis ~]# _
CTRL DERECHA